Capítulo 5 - Gestión de identidades y accesos (IAM)

Este capítulo cubre los siguientes tópicos:

- **Proceso de control de acceso : los** conceptos discutidos incluyen los pasos del proceso de control de acceso.
- **Acceso físico y lógico a los activos : los** conceptos discutidos incluyen la administración del control de acceso, el acceso a la información, el acceso a los sistemas, el acceso a los dispositivos y el acceso a las instalaciones.
- **Conceptos de identificación y autenticación : los** conceptos discutidos incluyen factores de conocimiento, factores de propiedad, factores característicos, factores de ubicación, factores de tiempo, autenticación de uno o varios factores y autenticación de dispositivo.
- **Implementación de identificación y autenticación : los** conceptos discutidos incluyen separación de deberes, privilegio mínimo / necesidad de saber, acceso predeterminado a sin acceso, servicios de directorio, inicio de sesión único, administración de identidad federada, administración de sesiones, registro y prueba de identidad, sistemas de administración de credenciales y responsabilidad.
- **Implementación de la identidad como servicio (IDaaS) :** describe las consideraciones al implementar IDaaS.
- **Integración de** servicios de identidad de terceros **:** detalla cómo integrar los servicios de identidad de terceros en una empresa, incluidos los servicios de identidad local, en la nube y federados.
- **Mecanismos de autorización :** cubre permisos, derechos y privilegios; modelos de control de acceso; y políticas de control de acceso.

- **Ciclo de vida de aprovisionamiento :** describe el ciclo de vida de aprovisionamiento, la administración de identidades y cuentas, la revisión del acceso a la cuenta del sistema y del usuario y la revocación de la cuenta.
- **Amenazas de control de acceso : los** conceptos discutidos incluyen amenazas de contraseña, amenazas de ingeniería social, DoS / DDoS, desbordamiento de búfer, código móvil, software malicioso, suplantación de identidad, rastreo y escucha clandestina, emanación, puerta trasera / trampilla, agregación de acceso y amenaza persistente avanzada (APT).
- **Prevenir o mitigar las amenazas de control de acceso :** describe formas de prevenir o mitigar las amenazas de control de acceso.

La gestión de identidades y accesos (IAM) se ocupa principalmente de controlar el acceso a los activos y gestionar las identidades. Estos activos incluyen computadoras, equipos, redes y aplicaciones. Los profesionales de la seguridad deben comprender cómo controlar el acceso físico y lógico a los activos y administrar los sistemas de identificación, autenticación y autorización. Por último, se deben abordar las amenazas del control de acceso.

La administración de identidad y acceso implica cómo funciona la administración de acceso, por qué la administración de identidad y acceso (IAM) es importante y cómo los componentes y dispositivos de IAM funcionan juntos en una empresa. El control de acceso permite que solo los usuarios, las aplicaciones, los dispositivos y los sistemas autorizados accedan a los recursos y la información de la empresa. Incluye instalaciones, sistemas de apoyo, sistemas de información, dispositivos de red y personal. Los profesionales de la seguridad utilizan los controles de acceso para especificar qué usuarios pueden acceder a un recurso, a qué recursos se puede acceder, qué operaciones se pueden realizar y qué acciones se supervisarán. Una vez más, la tríada CIA es importante para proporcionar IAM empresarial.

Table of Contents

Proceso de control de acceso 3
Identificar recursos 4
Identificar usuarios 4
Identificar las relaciones entre recursos y usuarios 5
Acceso físico y lógico a los activos 6
Administración de control de acceso 7
Centralizado 7
Descentralizado 7
Información 8
Sistemas 9
Dispositivos 9
Instalaciones 10
Conceptos de identificación y autenticación 11
Implementación de identificación y autenticación 36
Implementación de la identidad como servicio (IDaaS) 53
Integración de servicios de identidad de terceros 54
Mecanismos de autorización 55
Permisos, derechos y privilegios 55
Ciclo de vida de aprovisionamiento 66
Amenazas de control de acceso 70
Prevenir o mitigar las amenazas de control de acceso 79
Tareas de preparación de exámenes 80
Responder preguntas de revisión 85
Respuestas y explicaciones 89

Proceso de control de acceso

Aunque se han diseñado muchos enfoques para implementar controles de acceso, todos los enfoques generalmente implican los siguientes pasos:

1. Identifica recursos.
2. Identificar usuarios.
3. Identificar las relaciones entre los recursos y los usuarios.

Identificar recursos

Este primer paso en el proceso de control de acceso implica definir todos los recursos en la infraestructura de TI al decidir qué entidades deben protegerse. Al definir estos recursos, también debe considerar cómo se accederá a los recursos. Las siguientes preguntas se pueden utilizar como punto de partida durante la identificación de recursos:

- ¿El público en general accederá a esta información?
- ¿Debería restringirse el acceso a esta información solo a los empleados?
- ¿Debería restringirse el acceso a esta información a un subconjunto más pequeño de empleados?

Tenga en cuenta que los datos, las aplicaciones, los servicios, los servidores y los dispositivos de red se consideran recursos. Los recursos son cualquier activo organizacional al que los usuarios pueden acceder. En el control de acceso, los recursos a menudo se denominan objetos.

Identificar usuarios

Después de identificar los recursos, una organización debe identificar a los usuarios que necesitan acceso a los recursos. También se pueden identificar dispositivos y servicios que necesitarán acceso a recursos. Un profesional de seguridad típico debe administrar varios niveles de usuarios que requieren acceso a los recursos de la organización. Durante este paso, solo es importante identificar a los usuarios, dispositivos y

servicios. El nivel de acceso que se les dará a estos usuarios se analizará más a fondo en el siguiente paso. En el control de acceso, los usuarios, dispositivos y servicios a menudo se denominan sujetos.

Como parte de este paso, debe analizar y comprender las necesidades de los usuarios y luego medir la validez de esas necesidades frente a las necesidades organizativas, las políticas, los problemas legales, la sensibilidad de los datos y el riesgo.

Recuerde que cualquier estrategia de control de acceso y el sistema implementado para hacerla cumplir deben evitar la complejidad. Cuanto más complejo es un sistema de control de acceso, más difícil es administrarlo. Además, anticipar los problemas de seguridad que podrían ocurrir en sistemas más complejos es mucho más difícil. Como profesionales de la seguridad, debemos equilibrar las necesidades y políticas de seguridad de la organización con las necesidades de los usuarios. Si un mecanismo de seguridad que implementamos causa demasiada dificultad para el usuario, el usuario puede involucrarse en prácticas que subvierten los mecanismos que implementamos. Por ejemplo, si implementa una política de contraseñas que requiere una contraseña muy larga y compleja, los usuarios pueden encontrar difícil recordar sus contraseñas. Los usuarios pueden escribir sus contraseñas en notas adhesivas que se adjuntan a su monitor o teclado.

Identificar las relaciones entre recursos y usuarios

El paso final en el proceso de control de acceso es definir los niveles de control de acceso que deben existir para cada recurso y las relaciones entre los recursos y los usuarios, dispositivos y servicios. Por ejemplo, si una organización ha definido un servidor web como un recurso, los empleados generales pueden necesitar un nivel de acceso al recurso menos restrictivo que el público y un nivel de acceso al recurso más restrictivo que el personal de desarrollo web. Además, el servicio web puede necesitar acceso a ciertos recursos para proporcionar a los clientes los datos adecuados. Los controles de acceso deben diseñarse para

respaldar la funcionalidad comercial de los recursos que se están protegiendo. Controlar las acciones que se pueden realizar para un recurso específico en función de la función de un usuario, dispositivo o servicio es vital.

Acceso físico y lógico a los activos

El control de acceso consiste en utilizar controles físicos o lógicos para controlar quién o qué tiene acceso a una red, sistema o dispositivo. También involucra qué tipo de acceso se le da a la información, red, sistema, dispositivo o instalación. El control de acceso se proporciona principalmente mediante controles físicos y lógicos.

Nota

Los controles de acceso físico y lógico se tratan con más profundidad en el Capítulo 1 , " Gestión de riesgos y seguridad ".

El acceso físico se centra en controlar el acceso a una red, sistema o dispositivo. En la mayoría de los casos, el acceso físico implica el uso de control de acceso para evitar que los usuarios puedan tocar componentes de red (incluido el cableado), sistemas o dispositivos. Si bien las cerraduras son el método de control de acceso físico más popular para prevenir el acceso a dispositivos en un centro de datos, también se deben considerar otros controles físicos, como guardias y biometría, según las necesidades de la organización y el valor del activo que se protege. .

Los controles lógicos limitan el acceso que tiene un usuario a través de componentes de software o hardware. La autenticación y el cifrado son ejemplos de controles lógicos.

Al instalar un sistema de control de acceso, los profesionales de seguridad deben comprender quién necesita acceder al activo que se está protegiendo y cómo esos usuarios necesitan acceder al activo. Cuando varios usuarios necesitan acceder a un activo, la organización debe

configurar un sistema de control de acceso multicapa. Por ejemplo, es posible que los usuarios que deseen acceder al edificio solo necesiten registrarse con un guardia de seguridad. Sin embargo, para acceder al centro de datos cerrado dentro del mismo edificio, los usuarios necesitarían una tarjeta inteligente. Ambos serían controles de acceso físico. Para proteger los datos en un solo servidor dentro del edificio (pero no en el centro de datos), la organización necesitaría implementar mecanismos tales como autenticación, cifrado y listas de control de acceso (ACL) como controles de acceso lógico, pero también podría colocar el servidor en una sala de servidores cerrada para proporcionar control de acceso físico.

Al implementar controles de acceso físicos y lógicos, los profesionales de seguridad deben comprender los métodos de administración del control de acceso y los diferentes activos que deben protegerse y sus posibles controles de acceso.

Administración de control de acceso

La administración del control de acceso se produce de dos formas básicas: centralizada y descentralizada.

Centralizado

En el control de acceso centralizado, un departamento o personal central supervisa el acceso de todos los recursos de la organización. Este método de administración garantiza que el acceso de los usuarios se controle de manera coherente en toda la empresa. Sin embargo, este método puede ser lento porque todas las solicitudes de acceso son procesadas por la entidad central.

Descentralizado

En el control de acceso descentralizado, el personal más cercano a los recursos, como los gerentes de departamento y los propietarios de datos, supervisa el control de acceso de los recursos individuales. Este método

de administración asegura que quienes conocen los datos controlan los derechos de acceso a los mismos. Sin embargo, este método puede ser difícil de administrar porque no solo una entidad es responsable de configurar los derechos de acceso, perdiendo así la uniformidad y equidad de la seguridad.

Algunas empresas pueden implementar un enfoque híbrido que incluye control de acceso tanto centralizado como descentralizado. En este modelo de implementación, la administración centralizada se utiliza para el acceso básico, pero el propietario de los datos maneja el acceso granular a los activos individuales, como los datos en un servidor departamental.

Información

Para proteger completamente la información que se almacena en la red, los servidores u otros dispositivos de una organización, los profesionales de seguridad deben proporcionar controles de acceso tanto físicos como lógicos. Los controles de acceso físico, como colocar dispositivos en una habitación cerrada con llave, protegen los dispositivos en los que reside la información. Los controles de acceso lógico, como la implementación de datos o el cifrado de unidades, el cifrado de transporte, las ACL y los firewalls, protegen los datos del acceso no autorizado.

El valor de la información protegida probablemente determinará los controles que una organización está dispuesta a implementar. Por ejemplo, la correspondencia regular en una computadora cliente probablemente no requerirá los mismos controles que los datos financieros almacenados en un servidor. Para la computadora cliente, la organización puede simplemente implementar un firewall de software local y los permisos de ACL apropiados en las carpetas y archivos locales. Para el servidor, es posible que la organización deba implementar medidas más complejas, incluido el cifrado de unidades, el cifrado de transporte, las ACL y otras medidas.

Sistemas

Para proteger completamente los sistemas utilizados por la organización, incluidos los equipos cliente y servidor, los profesionales de la seguridad pueden depender de controles de acceso tanto físicos como lógicos. Sin embargo, algunos sistemas, como las computadoras cliente, pueden implementarse de tal manera que solo se utilicen controles físicos mínimos. Si a un usuario se le concede acceso a un edificio, es posible que encuentre computadoras cliente en cubículos no seguros.en todo el edificio. Para estos sistemas, un profesional de la seguridad debe asegurarse de que se implementen los mecanismos de autenticación adecuados. Si se almacena información confidencial en los equipos cliente, también se debe implementar el cifrado. Pero solo la organización puede determinar mejor qué controles implementar en los equipos cliente individuales.

Cuando se trata de servidores, determinar qué controles de acceso implementar suele ser un proceso más complicado. Los profesionales de seguridad deben trabajar con el propietario del servidor, ya sea un jefe de departamento o un profesional de TI, para determinar el valor del activo y la protección necesaria. Por supuesto, la mayoría de los servidores deben colocarse en una habitación cerrada con llave. En muchos casos, será un centro de datos o una sala de servidores. Sin embargo, los servidores se pueden implementar en oficinas cerradas normales si es necesario. Además, se deben implementar otros controles para garantizar que el sistema esté completamente protegido. Las necesidades de control de acceso de un servidor de archivos son diferentes a las de un servidor web o un servidor de base de datos. Es vital que la organización realice una evaluación exhaustiva de los datos que se procesan y almacenan en el sistema antes de determinar qué controles de acceso implementar.

Dispositivos

Al igual que con los sistemas, la mejor forma de proporcionar acceso físico a los dispositivos es colocándolos en una habitación segura. El acceso

lógico a los dispositivos se proporciona mediante la implementación de la lista de reglas o ACL adecuada, la autenticación y el cifrado, así como la protección de las interfaces remotas que se utilizan para administrar el dispositivo. Además, los profesionales de la seguridad deben asegurarse de que las cuentas y contraseñas predeterminadas se cambien o deshabiliten en el dispositivo.

Para cualquier profesional de TI que necesite acceder al dispositivo, se debe configurar una cuenta de usuario para el profesional con el nivel adecuado de acceso necesario. Si se utiliza una interfaz remota, asegúrese de habilitar el cifrado, como SSL, para asegurarse de que la comunicación a través de la interfaz remota no sea interceptada y leída. Los profesionales de seguridad deben monitorear de cerca los anuncios de los proveedores de cualquier dispositivo para asegurarse de que los dispositivos se mantengan actualizados con los últimos parches de seguridad y actualizaciones de firmware.

Instalaciones

Con las instalaciones, la principal preocupación es el acceso físico, que se puede proporcionar mediante cerraduras, cercas, bolardos, guardias y circuito cerrado de televisión (CCTV). Muchas organizaciones piensan que estas medidas son suficientes. Pero con los sistemas de control industrial avanzados de hoy y el Internet de las cosas (IoT), las organizaciones también deben considerar cualquier dispositivo involucrado en la seguridad de las instalaciones. Si una organización tiene un sistema de alarma / seguridad que permite el acceso de visualización remota desde Internet, la lógica adecuadaDeben existir controles para evitar que un usuario malintencionado acceda al sistema y cambie su configuración o que utilice el sistema para obtener información privilegiada sobre el diseño de las instalaciones y las operaciones diarias. Si la organización utiliza un sistema de control industrial (ICS), los controles lógicos también deben ser una prioridad. Los profesionales de seguridad deben trabajar con las organizaciones para garantizar que los controles físicos y lógicos se

implementen de manera adecuada para garantizar que toda la instalación esté protegida.

Conceptos de identificación y autenticación

Para poder acceder a un recurso, un usuario, dispositivo o servicio debe profesar una identidad, proporcionar las credenciales necesarias y tener los derechos adecuados para realizar las tareas que se deben completar. El primer paso en este proceso se llama *identificación* , que es el acto de un usuario, dispositivo o servicio que profesa una identidad a un sistema de control de acceso.

La autenticación , la segunda parte del proceso, es el acto de validar a un usuario, dispositivo o servicio con un identificador único al proporcionar las credenciales adecuadas. Al intentar diferenciar entre los dos, los profesionales de la seguridad deben saber que la identificación identifica al usuario, dispositivo o servicio y la autenticación verifica que la identidad proporcionada por el usuario, dispositivo o servicio es válida. La autenticación generalmente se implementa a través de una contraseña proporcionada al iniciar sesión. Cuando un usuario, dispositivo o servicio inicia sesión en un sistema, el proceso de inicio de sesión debe validar el inicio de sesión después de que el usuario, dispositivo o servicio proporcione todos los datos de entrada.

Después de que se autentica un usuario, dispositivo o servicio, se deben otorgar al usuario, dispositivo o servicio los derechos y permisos sobre los recursos. El proceso se conoce como *autorización* .

Las formas más populares de identificación de usuario incluyen ID de usuario o cuentas de usuario, números de cuenta y números de identificación personal (PIN).

NIST SP 800-63

La publicación especial NIST (SP) 800-63 proporciona un conjunto de requisitos técnicos para las agencias federales que implementan servicios de identidad digital, incluida una descripción general de los marcos de identidad; utilizando autenticadores, credenciales y afirmaciones en sistemas digitales. En julio de 2017, NIST finalizó el SP 800-63 de cuatro volúmenes titulado "Pautas de identidad digital". Los cuatro volúmenes de este SP son los siguientes:

- **SP 800-63 Pautas de identidad digital:** proporciona la metodología de evaluación de riesgos y una descripción general de los marcos de identidad generales, utilizando autenticadores, credenciales y afirmaciones juntos en un sistema digital y un proceso basado en el riesgo de selección de niveles de garantía. SP 800-63 contiene material tanto normativo como informativo.
- **SP 800-63A Enrollment and Identity Proofing:** Aborda cómo los solicitantes pueden probar sus identidades y convertirse en sujetos válidos dentro de un sistema de identidad. Proporciona requisitos para los procesos mediante los cuales los solicitantes pueden probar e inscribirse en uno de los tres niveles diferentes de mitigación de riesgos en escenarios remotos y físicamente presentes. SP 800-63A contiene material tanto normativo como informativo.
- **SP 800-63B Autenticación y administración del ciclo de vida:** aborda cómo una persona puede autenticarse de manera segura ante un proveedor de servicios de credenciales (CSP) para acceder a un servicio digital o un conjunto de servicios digitales. Este volumen también describe el proceso de vincular un autenticador a una identidad. SP 800-63B contiene material tanto normativo como informativo.
- **SP 800-63C Federación y afirmaciones:** proporciona requisitos sobre el uso de arquitecturas de identidad federada y afirmaciones para transmitir los resultados de los procesos de autenticación y la información de identidad relevante a una aplicación de agencia. Además, este volumen ofrece técnicas de mejora de la privacidad para compartir información sobre un sujeto válido y autenticado, y

describe métodos que permiten una autenticación multifactor sólida (MFA) mientras el sujeto permanece seudónimo para el servicio digital. SP 800-63C contiene material tanto normativo como informativo.

Específicamente en SP 800-63B, las contraseñas entran en la categoría de secretos memorizados. Se dan pautas de secreto memorizado y otras contraseñas que pueden o no diferir mucho de las que se dieron en el pasado y que seguimos hoy:

- Los secretos memorizados deben tener al menos 8 caracteres de longitud si los elige el suscriptor o al menos 6 caracteres de longitud si el CSP o el verificador los elige al azar.
- Los verificadores deben exigir que los secretos memorizados elegidos por el suscriptor tengan al menos 8 caracteres de longitud y se les debe permitir incluir todos los caracteres ASCII impresos, el espacio y los caracteres Unicode.
- Los secretos memorizados que son elegidos aleatoriamente por el CSP o por el verificador deben tener al menos 6 caracteres de longitud y deben generarse utilizando un generador de bits aleatorios aprobado.
- Los verificadores secretos memorizados no deben permitir que el suscriptor almacene una "pista" que sea accesible para un reclamante no autenticado. Los verificadores no deben instar a los suscriptores a utilizar tipos específicos de información (por ejemplo, "¿Cómo se llamaba su primera mascota?") Al elegir secretos memorizados.
- Al procesar solicitudes para establecer y cambiar secretos memorizados, los verificadores deben comparar los secretos potenciales con una lista que contenga valores que se sabe que se usan comúnmente, se esperan o se comprometen. Por ejemplo, la lista PUEDE incluir, pero no se limita a, contraseñas obtenidas de corporaciones de infracción anteriores, palabras de diccionario, caracteres repetitivos o secuenciales (por ejemplo, "aaaaaa" o

"1234abcd") y palabras específicas del contexto, como el nombre del servicio, el nombre de usuario y derivados del mismo.

- Los verificadores deben ofrecer orientación al suscriptor, como un medidor de seguridad de la contraseña, para ayudar al usuario a elegir un secreto fuerte memorizado.
- Los verificadores deben implementar un mecanismo de limitación de velocidad que limite efectivamente el número de intentos fallidos de autenticación que se pueden realizar en la cuenta del suscriptor.
- Los verificadores no deben imponer otras reglas de composición (p. Ej., Exigir mezclas de diferentes tipos de caracteres o prohibir caracteres repetidos consecutivamente) para los secretos memorizados. Los verificadores no deben exigir que los secretos memorizados se modifiquen arbitrariamente (por ejemplo, periódicamente). Sin embargo, los verificadores deben forzar un cambio si hay evidencia de compromiso del autenticador.
- Los verificadores deben permitir que los solicitantes utilicen la función "pegar" al ingresar un secreto memorizado, facilitando así el uso de administradores de contraseñas, que se utilizan ampliamente y en muchos casos aumentan la probabilidad de que los usuarios elijan secretos memorizados más fuertes.
- Para ayudar al reclamante a ingresar con éxito un secreto memorizado, el verificador debe ofrecer una opción para mostrar el secreto, en lugar de una serie de puntos o asteriscos, hasta que se ingrese.
- El verificador debe utilizar encriptación aprobada y un canal protegido autenticado cuando solicite secretos memorizados para brindar resistencia a escuchas y ataques de intermediarios.
- Los verificadores deben almacenar los secretos memorizados en una forma que sea resistente a los ataques fuera de línea. Los secretos memorizados deben salarse y procesarse mediante una función de derivación de clave unidireccional adecuada. La sal debe tener al menos 32 bits de longitud y elegirse arbitrariamente para minimizar las colisiones de valores de sal entre los valores hash almacenados.

> Tanto el valor de sal como el hash resultante deben almacenarse para cada suscriptor utilizando un autenticador secreto memorizado.

According to NIST SP 800-63B, passwords remain a very widely used form of authentication despite widespread frustration with the use of passwords from both a usability and security standpoint. Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose passwords that can be easily guessed. To address the resultant security concerns, online services han introducido reglas en un esfuerzo por aumentar la complejidad de estos secretos memorizados. La forma más notable de estas son las reglas de composición, que requieren que el usuario elija contraseñas construidas con una combinación de tipos de caracteres, como al menos un dígito, una letra mayúscula y un símbolo. Sin embargo, los análisis de las bases de datos de contraseñas violadas revelan que el beneficio de tales reglas no es tan significativo como se pensaba inicialmente, aunque el impacto en la usabilidad y la memorización es severo. En SP 800-63B se presenta un enfoque diferente y algo más simple, basado principalmente en la longitud de la contraseña.

Muchos ataques asociados con el uso de contraseñas no se ven afectados por la complejidad y longitud de las contraseñas. Los ataques de registro de pulsaciones de teclas, suplantación de identidad (phishing) e ingeniería social son igualmente efectivos en contraseñas largas y complejas que en contraseñas simples.

Se ha descubierto que la longitud de la contraseña es un factor principal para caracterizar la seguridad de la contraseña. Las contraseñas que son demasiado cortas ceden a los ataques de fuerza bruta, así como a los ataques de diccionario que utilizan palabras y contraseñas comúnmente elegidas.

La longitud mínima de la contraseña que debe requerirse depende en gran medida del modelo de amenaza que se está abordando. Los ataques

en línea en los que el atacante intenta iniciar sesión adivinando la contraseña se pueden mitigar limitando la tasa de intentos de inicio de sesión permitidos. Para evitar que un atacante (o un demandante persistente con habilidades de mecanografía deficientes) inflija fácilmente un ataque de denegación de servicio al suscriptor al realizar muchas suposiciones incorrectas, las contraseñas deben ser lo suficientemente complejas como para que la limitación de velocidad no se produzca después de un número modesto de intentos erróneos, pero ocurre antes de que haya una posibilidad significativa de una suposición exitosa.

Se debe alentar a los usuarios a que hagan sus contraseñas tan largas como quieran, dentro de lo razonable. Dado que el tamaño de una contraseña con hash es independiente de su longitud, no hay razón para no permitir el uso de contraseñas largas (o frases de contraseña) si el usuario lo desea. Las contraseñas extremadamente largas (quizás megabytes de longitud) posiblemente requieran un tiempo de procesamiento excesivo para el hash, por lo que es razonable tener algún límite.

Las reglas de composición se utilizan comúnmente en un intento de aumentar la dificultad de adivinar las contraseñas elegidas por el usuario. La investigación ha demostrado, sin embargo, que los usuarios responden de formas muy predecibles a los requisitos impuestos por las reglas de composición. Por ejemplo, es relativamente probable que un usuario que haya elegido "contraseña" como contraseña elija "Contraseña1" si se le solicita que incluya una letra mayúscula y un número, o "¡Contraseña1!" si también se requiere un símbolo.

Los usuarios también expresan su frustración cuando los servicios en línea rechazan los intentos de crear contraseñas complejas. Muchos servicios rechazan las contraseñas con espacios y varios caracteres especiales. En algunos casos, los caracteres especiales que no se aceptan pueden ser un esfuerzo por evitar ataques, como la inyección SQL, que dependen de esos caracteres. Pero una contraseña correctamente hash no se enviaría intacta a una base de datos en ningún caso, por lo que tales precauciones

son innecesarias. Los usuarios también deben poder incluir espacios para permitir el uso de frases. Los espacios en sí mismos, sin embargo, añaden poco a lacomplejidad de las contraseñas y puede introducir problemas de usabilidad (por ejemplo, el uso no detectado de dos espacios en lugar de uno), por lo que puede ser beneficioso eliminar los espacios repetidos en las contraseñas escritas antes de la verificación.

Users' password choices are very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as the "Password1!" example above. For this reason, it is recommended that passwords chosen by users be compared against a "black list" of unacceptable passwords. This list should include passwords from previous breach corpuses, dictionary words, and specific words (such as the name of the service itself) that users are likely to choose. Since user choice of passwords will also be governed by a minimum length requirement, this dictionary need only include entries meeting that requirement.

Los secretos memorizados altamente complejos introducen una nueva vulnerabilidad potencial: es menos probable que sean memorables y es más probable que se escriban o almacenen electrónicamente de manera insegura. Si bien estas prácticas no son necesariamente vulnerables, estadísticamente sí lo serán algunos métodos para registrar tales secretos. Esta es una motivación adicional para no requerir secretos memorizados excesivamente largos o complejos.

Otro factor que determina la fuerza de los secretos memorizados es el proceso mediante el cual se generan. Los secretos elegidos al azar (en la mayoría de los casos por el verificador o el CSP) y distribuidos uniformemente serán más difíciles de adivinar o de un ataque de fuerza bruta que los secretos elegidos por el usuario que cumplan los mismos requisitos de longitud y complejidad.

Cinco factores para la autenticación

Después de establecer el método de identificación de usuario, dispositivo o servicio, una organización debe decidir qué método de autenticación utilizar.

Los métodos de autenticación se dividen en cinco categorías amplias:

- **Autenticación del factor de conocimiento:** algo que una persona sabe
- **Autenticación del factor de propiedad:** algo que una persona tiene o posee
- **Autenticación de factores característicos:** algo que una persona es
- **Autenticación del factor de ubicación: en** algún lugar
- **Autenticación de factor de tiempo:** el tiempo que una persona se autentica

Nota

Originalmente había tres factores (algo que sabes, algo que tienes y algo que eres). Se los denominó factores de Tipo I, Tipo II y Tipo III, respectivamente. Sin embargo, la tecnología moderna ha obligado al campo de la seguridad a reconocer recientemente dos factores adicionales: el lugar en el que se encuentra y el momento de la autenticación.

Factores de conocimiento

Como se describe brevemente en la sección anterior, la autenticación del *factor de conocimiento* es la autenticación que se proporciona en función de algo que una persona sabe. Aunque la forma más popular de autenticación utilizada por esta categoría es la autenticación de contraseña, se pueden usar otros factores de conocimiento, incluida la fecha de nacimiento, el apellido de soltera de la madre, la combinación de teclas o el PIN.

Tipos y administración de contraseñas

Como se mencionó anteriormente, la autenticación de contraseña es el método de autenticación más popular implementado en la actualidad. Sin embargo, los tipos de contraseña pueden variar de un sistema a otro. Es fundamental comprender todos los tipos de contraseñas que se pueden utilizar. Las contraseñas y otros factores de conocimiento se denominan secretos memorizados en NIST SP 800-63.

Los tipos de contraseñas con las que debería estar familiarizado incluyen

- **Palabra estándar o contraseñas simples:** como su nombre lo indica, estas contraseñas consisten en palabras simples que a menudo incluyen una combinación de letras mayúsculas y minúsculas y números. La ventaja de este tipo de contraseña es que es fácil de recordar. Una desventaja de este tipo de contraseña es que es fácil de descifrar o romper para los atacantes, lo que da como resultado una cuenta comprometida.
- **Combinación de contraseñas:** este tipo de contraseña utiliza una combinación de palabras del diccionario, generalmente dos palabras no relacionadas. También se denominan contraseñas de composición. Al igual que las contraseñas de palabras estándar, pueden incluir letras y números en mayúsculas y minúsculas. Una ventaja de esta contraseña es que es más difícil de romper que las contraseñas simples. Una desventaja es que puede ser difícil de recordar.
- **Contraseñas estáticas:** este tipo de contraseña es el mismo para cada inicio de sesión. Proporciona un nivel mínimo de seguridad porque la contraseña nunca cambia. Se ve con mayor frecuencia en redes peer-to-peer.
- **Contraseñas complejas:** este tipo de contraseña obliga al usuario a incluir una combinación de letras mayúsculas y minúsculas,

números y caracteres especiales. Hoy en día, para muchas organizaciones, este tipo de contraseña se aplica como parte de la política de contraseñas de la organización. Una ventaja de este tipo de contraseña es que es muy difícil de descifrar. Una desventaja es que es más difícil de recordar y, a menudo, puede ser mucho más difícil ingresar correctamente que las contraseñas estándar o combinadas.

- **Contraseñas de** frase de **contraseña:** este tipo de contraseña requiere que se utilice una frase larga. Debido a la longitud de la contraseña, es más fácil de recordar pero mucho más difícil de atacar, y ambas son ventajas definitivas. La incorporación de letras mayúsculas y minúsculas, números y caracteres especiales en este tipo de contraseña puede aumentar significativamente la seguridad de la autenticación.
- **Contraseñas cognitivas:** este tipo de contraseña es un dato que se puede utilizar para verificar la identidad de una persona. Esta información se proporciona al sistema respondiendo una serie de preguntas basadas en la vida del usuario, como el color favorito, el nombre de la mascota, el apellido de soltera de la madre, etc. Una ventaja de este tipo es que los usuarios generalmente pueden recordar fácilmente esta información. La desventaja es que alguien que tenga un conocimiento íntimo de la vida de la persona (cónyuge, hijo, hermano, etc.) también podría proporcionar esta información.
- **Contraseñas de un solo uso:** también llamada contraseña dinámica, este tipo de contraseña solo se usa una vez para iniciar sesión en el sistema de control de acceso. Este tipo de contraseña proporciona el nivel más alto de seguridad porque las contraseñas se descartan cuando se utilizan.
- **Contraseñas gráficas:** también llamada CAPTCHA, que significa prueba de Turing pública completamente automatizada para distinguir entre computadoras y humanos, contraseñas, este tipo de contraseña utiliza gráficos como parte del mecanismo de autenticación. Una implementación popular requiere que el usuario

ingrese una serie de caracteres en el gráfico mostrado. Esta implementación asegura que un humano ingrese la contraseña, no un robot. Otra implementación popular requiere que el usuario seleccione el gráfico apropiado para su cuenta de una lista de gráficos dada.

- **Contraseñas numéricas:** este tipo de contraseña incluye solo números. Tenga en cuenta que las opciones de una contraseña están limitadas por la cantidad de dígitos permitidos. Por ejemplo, si todas las contraseñas son de 4 dígitos, entonces el número máximo de posibilidades de contraseña es 10,000, de 0000 a 9999. Una vez que un atacante se da cuenta de que solo se usan números, descifrar las contraseñas de los usuarios sería mucho más fácil porque se conocerían las posibilidades.

Las contraseñas se consideran más débiles que las frases de contraseña, las contraseñas de un solo uso, los dispositivos token y las frases de inicio de sesión. Una vez que una organización ha decidido qué tipo de contraseña utilizar, la organización debe establecer sus políticas de administración de contraseñas.

Las consideraciones sobre la administración de contraseñas incluyen, entre otras,

- **Duración de la contraseña:** cuánto tiempo será válida la contraseña. Para la mayoría de las organizaciones, las contraseñas tienen una validez de 60 a 90 días.
- **Historial de contraseñas:** cuánto tiempo antes de que se pueda reutilizar una contraseña. Las políticas de contraseñas suelen recordar una cierta cantidad de contraseñas utilizadas anteriormente.

- **Período de autenticación:** cuánto tiempo puede permanecer un usuario conectado. Si un usuario permanece conectado durante el período sin actividad, se cerrará automáticamente la sesión.
- **Complejidad de la contraseña:** cómo se estructurará la contraseña. La mayoría de las organizaciones requieren letras mayúsculas y minúsculas, números y caracteres especiales.
- **Longitud de la contraseña: la longitud que** debe tener la contraseña. La mayoría de las organizaciones requieren de 8 a 12 caracteres.
- **Enmascaramiento de contraseña:** evita que se aprenda una contraseña a través de la navegación lateral al ocultar los caracteres ingresados excepto el último.

Como parte de la gestión de contraseñas, las organizaciones deben establecer un procedimiento para cambiar las contraseñas. La mayoría de las organizaciones implementan un servicio que permite a los usuarios restablecer automáticamente su contraseña antes de que expire. Además, la mayoría de las organizaciones deberían considerar establecer una política de restablecimiento de contraseña en los casos en que los usuarios hayan olvidado su contraseña o se hayan visto comprometidas. Un enfoque de autoservicio de restablecimiento de contraseñas permite a los usuarios restablecer sus propias contraseñas sin la ayuda de los empleados de la mesa de ayuda. Un enfoque de restablecimiento de contraseña asistido requiere que los usuarios se comuniquen con el personal de la mesa de ayuda para obtener ayuda para cambiar sus contraseñas.

Las políticas de restablecimiento de contraseña también pueden verse afectadas por otras políticas organizativas, como las políticas de bloqueo de cuentas. Las políticas de bloqueo de cuentas son políticas de seguridad que implementan las organizaciones para protegerse contra los ataques que se llevan a cabo contra las contraseñas. Las organizaciones a menudo configuran políticas de bloqueo de cuentas para que las cuentas de usuario se bloqueen después de una cierta cantidad de intentos fallidos

de inicio de sesión. Si una cuenta está bloqueada, es posible que el administrador del sistema deba desbloquear o volver a habilitar la cuenta de usuario. Los profesionales de la seguridad también deben considerar alentar a las organizaciones a exigir a los usuarios que restablezcan su contraseña si su cuenta se ha bloqueado o después de que se haya utilizado una contraseña durante un cierto período de tiempo (90 días para la mayoría de las organizaciones). Para la mayoría de las organizaciones, todas las políticas de contraseñas, incluidas las políticas de bloqueo de cuentas, se implementan a nivel empresarial en los servidores que administran la red. Las políticas de bloqueo de cuentas se utilizan con mayor frecuencia para proteger contra ataques de diccionario o de fuerza bruta.

Nota

Un término más antiguo con el que es posible que deba estar familiarizado es el *nivel de recorte* . Un nivel de recorte es un umbral de referencia configurado por encima del cual se registrarán las infracciones. Por ejemplo, una organización puede querer comenzar a registrar cualquier intento de inicio de sesión fallido después del primero, y el bloqueo de la cuenta se produce después de cinco intentos fallidos. Esto se conoce como limitación de frecuencia en NIST SP 800-63, que se analiza más adelante en este capítulo.

Dependiendo de los servidores que se utilicen para administrar la empresa, los profesionales de seguridad deben conocer los problemas de seguridad que afectan la administración de cuentas de usuario y contraseñas. Dos sistemas operativos de servidor populares son Linux y Windows.

Para Linux, las contraseñas se almacenan en el *archivo / etc / passwd* o */ etc / shadow* . Debido a que el *archivo / etc / passwd* es un archivo de texto al que se puede acceder fácilmente, debe asegurarse de que cualquier servidor Linux use el *archivo / etc / shadow* , donde las contraseñas del archivo se pueden proteger mediante un hash. El usuario

root en Linux es una cuenta predeterminada a la que se le otorga acceso de nivel administrativo a todo el servidor. Si la cuenta de *root se* ve comprometida, se deben cambiar todas las contraseñas. El acceso a la cuenta de *root* debe estar limitado solo a los administradores del sistema, y el inicio de sesión de root solo debe permitirse a través de una consola del sistema local, no de forma remota.

Para equipos con Windows que están en grupos de trabajo, el Administrador de cuentas de seguridad (SAM) almacena las contraseñas de los usuarios en formato hash. Sin embargo, existen problemas de seguridad conocidos con un SAM, incluida la capacidad de volcar los hashes de contraseña directamente desde el registro. Debe tomar todas las medidas de seguridad recomendadas por Microsoft para proteger este archivo. Si administra una red de Windows, debe cambiar el nombre de la cuenta de administrador predeterminada o deshabilitarla. Si conserva esta cuenta, asegúrese de asignarle una contraseña. La cuenta de administrador predeterminada puede tener acceso completo a un servidor de Windows.

Factores de propiedad

La autenticación del factor de propiedad es la autenticación que se proporciona en función de algo que tiene una persona. Los factores de propiedad pueden incluir dispositivos token, tarjetas de memoria, teléfonos, llaves, llaveros y tarjetas inteligentes.

Dispositivos token síncronos y asincrónicos

El dispositivo de token (a menudo denominado generador de contraseñas) es un dispositivo de mano que presenta al servidor de autenticación la contraseña de un solo uso. Si el método de autenticación requiere un dispositivo token, el usuario debe estar en posesión física del dispositivo para autenticarse. Entonces, aunque el dispositivo de token proporciona una contraseña al servidor de autenticación, el dispositivo de token se considera un factor de autenticación de propiedad porque su uso requiere la propiedad del dispositivo.

Se utilizan dos métodos básicos de autenticación de dispositivos token: síncrono o asíncrono. Un token síncrono genera una contraseña única a intervalos de tiempo fijos con el servidor de autenticación. Un token asincrónico genera la contraseña basada en una técnica de desafío / respuesta con el servidor de autenticación, y el dispositivo de token proporciona la respuesta correcta al desafío del servidor de autenticación.

Un dispositivo de token generalmente solo se implementa en entornos muy seguros debido al costo de implementar el dispositivo de token. Además, las soluciones basadas en tokens pueden experimentar problemas debido a la vida útil de la batería del dispositivo token.

Tarjetas de memoria

Una tarjeta de memoria es una tarjeta magnética que se emite a usuarios válidos. La tarjeta contiene información de autenticación del usuario. Cuando se pasa la tarjeta por un lector de tarjetas, la información almacenada en la tarjeta se compara con la información que ingresa el usuario. Si la información coincide, el servidor de autenticación aprueba el inicio de sesión. Si no coincide, se deniega la autenticación.

Debido a que la tarjeta debe ser leída por un lector de tarjetas, cada computadora o dispositivo de acceso debe tener su propio lector de tarjetas. Además, las tarjetas deben crearse y programarse. Ambos pasos agregan complejidad y costo al proceso de autenticación. Sin embargo, a menudo vale la pena la complejidad y el costo adicionales por la seguridad adicional que proporciona, que es un beneficio definitivo de este sistema. Sin embargo, los datos de las tarjetas de memoria no están protegidos, una debilidad que las organizaciones deben considerar antes de implementar este tipo de sistema. Las tarjetas de solo memoria son muy fáciles de falsificar.

Tarjetas inteligentes

Similar a una tarjeta de memoria, una tarjeta inteligente acepta, almacena y envía datos, pero puede contener más datos que una tarjeta

de memoria. Las tarjetas inteligentes, a menudo conocidas como tarjetas de circuito integrado (ICC), contienen memoria como una tarjeta de memoria, pero también contienen un chip integrado como tarjetas bancarias o de crédito. Las tarjetas inteligentes utilizan lectores de tarjetas. Sin embargo, el servidor de autenticación utiliza los datos de la tarjeta inteligente sin la intervención del usuario. Para protegerse contra tarjetas inteligentes perdidas o robadas, la mayoría de las implementaciones requieren que el usuario ingrese un PIN secreto, lo que significa que el usuario en realidad proporciona un factor de autenticación de conocimiento (PIN) y propiedad (tarjeta inteligente).

Se utilizan dos tipos básicos de tarjetas inteligentes: tarjetas de contacto y tarjetas sin contacto. Las tarjetas de contacto requieren contacto físico con el lector de tarjetas, generalmente deslizándolo. Las tarjetas sin contacto, también denominadas tarjetas de proximidad, simplemente deben estar muy cerca del lector. Hay disponibles tarjetas híbridas que permiten utilizar una tarjeta en sistemas con y sin contacto.

Para fines comparativos, los profesionales de la seguridad deben recordar que las tarjetas inteligentes tienen capacidad de procesamiento debido a los chips integrados. Las tarjetas de memoria no tienen capacidad de procesamiento. Los sistemas de tarjetas inteligentes son mucho más confiables que los sistemas de tarjetas de memoria.

Las tarjetas inteligentes son incluso más caras de implementar que las tarjetas de memoria. Muchas organizaciones prefieren las tarjetas inteligentes a las tarjetas de memoria porque son más difíciles de falsificar y los datos que contienen se pueden proteger mediante cifrado.

Factores característicos

La autenticación de factores característicos es la autenticación que se proporciona en función de algo que es una persona. La tecnología biométrica es la tecnología que permite a los usuarios autenticarse en función de características fisiológicas o de comportamiento. FisiológicoLas

características incluyen cualquier atributo físico único del usuario, incluidos el iris, la retina y las huellas dactilares. Las características de comportamiento miden las acciones de una persona en una situación, incluidos los patrones de voz y las características de entrada de datos.

Las tecnologías biométricas ahora son comunes en algunos de los sistemas operativos más populares. Los ejemplos incluyen Windows Hello y las tecnologías Touch ID y Face ID de Apple. Como profesional de la seguridad, debe conocer las nuevas tecnologías a medida que se implementan para brindar mayor seguridad. Educar a los usuarios sobre estas tecnologías también debe ser una prioridad para garantizar que los usuarios adopten estas tecnologías a medida que se implementan.

Características fisiológicas

Los sistemas fisiológicos utilizan un dispositivo de escaneo biométrico para medir cierta información sobre una característica fisiológica. Debe comprender los siguientes sistemas biométricos fisiológicos:

- Huella dactilar
- Lector dactilar
- Geometría de la mano
- Topografía de mano
- Escaneos de palma o mano
- Exploraciones faciales
- Escaneos de retina
- Escaneos de iris
- Exploraciones vasculares

Un escaneo de huellas dactilares generalmente escanea las crestas de un dedo para buscar coincidencias. Un tipo especial de escaneo de huellas dactilares llamado coincidencia de minucias es más microscópico porque registra las bifurcaciones y otras características detalladas. La coincidencia

de minucias requiere más espacio en el servidor de autenticación y más tiempo de procesamiento que los escaneos de huellas dactilares de cresta. Los sistemas de escaneo de huellas dactilares tienen una tasa de aceptación de usuario más baja que muchos sistemas porque a los usuarios les preocupa cómo se utilizará y compartirá la información de las huellas dactilares.

Un escaneo digital extrae solo ciertas características de una huella digital. Debido a que se necesita una cantidad limitada de información de huellas digitales, los escaneos digitales requieren menos espacio en el servidor o tiempo de procesamiento que cualquier tipo de escaneo de huellas digitales.

Un escaneo de la geometría de la mano generalmente obtiene el tamaño, la forma u otros atributos de diseño de la mano de un usuario, pero también puede medir la longitud del hueso o la longitud del dedo. Dos categorías de sistemas de geometría manual son los sistemas de detección mecánicos y de borde de imagen. Independientemente de la categoría que se utilice, los escáneres de geometría manual requieren menos espacio en el servidor y tiempo de procesamiento que los escáneres de huellas dactilares o dactilares.

Un escaneo de topografía manual registra los picos y valles de la mano y su forma. Este sistema generalmente se implementa junto con los escaneos de geometría manual porque los escaneos de topografía manual no son lo suficientemente únicos si se usan solos.

Un escaneo de la palma o de la mano combina tecnologías de huella dactilar y geometría de la mano. Registra la información de las huellas dactilares de cada dedo, así como la información de la geometría de la mano.

Un escaneo facial registra las características faciales, incluida la estructura ósea, el ancho de los ojos y el tamaño de la frente. Este método biométrico utiliza características propias o caras propias. Ninguno de

estos métodos captura realmente una imagen de un rostro. Con las características propias, se mide y registra la distancia entre los rasgos faciales. Con las caras propias, las medidas de los componentes faciales se recopilan y comparan con un conjunto de caras propias estándar. Por ejemplo, la cara de una persona puede estar compuesta por la cara promedio más 21% de la cara propia 1, 83% de la cara propia 2 y –18% de la cara propia 3. Muchos dispositivos biométricos de escaneo facial utilizarán una combinación de características propias y caras propias.

Una gammagrafía de retina explora el patrón de vasos sanguíneos de la retina. Una gammagrafía de retina se considera más intrusiva que una gammagrafía de iris.

Un escáner de iris escanea la parte coloreada del ojo, incluidas todas las fisuras, coronas y surcos. Los escáneres de iris tienen una precisión mayor que cualquier otro escaneo biométrico.

Una exploración vascular explora el patrón de las venas en la mano o la cara del usuario. Si bien este método puede ser una buena opción porque no es muy intrusivo, las lesiones físicas en la mano o el rostro, según el sistema que utilice, podrían provocar falsos rechazos.

Características de comportamiento

Los sistemas de comportamiento utilizan un dispositivo de escaneo biométrico para medir las acciones de una persona. Debe comprender los siguientes sistemas biométricos de comportamiento:

- Dinámica de la firma
- Dinámica de pulsaciones de teclas
- Patrón de voz o impresión

La dinámica de la firma mide la velocidad del trazo, la presión del lápiz y la aceleración y desaceleración mientras el usuario escribe su firma. La verificación dinámica de firma (DSV) analiza las características de la firma y las características específicas del proceso de firma.

La dinámica de pulsaciones de teclas mide el patrón de escritura que usa un usuario cuando ingresa una contraseña u otra frase predeterminada. En este caso, incluso si se ingresa la contraseña o frase correcta pero el patrón de ingreso en el teclado es diferente, se le negará el acceso al usuario. El tiempo de vuelo, un término asociado con la dinámica de pulsaciones de teclas, es la cantidad de tiempo que se tarda en cambiar entre teclas. El tiempo de permanencia es la cantidad de tiempo que mantiene presionada una tecla.

El patrón de voz o impresión mide el patrón de sonido de un usuario que dice una determinada palabra. Cuando el usuario intente autenticarse, se le pedirá que repita esas palabras en diferentes órdenes. Si el patrón coincide, se permite la autenticación.

Consideraciones biométricas

Al considerar las tecnologías biométricas, los profesionales de la seguridad deben comprender los siguientes términos:

- **Tiempo de inscripción:** El proceso de obtención de la muestra que utiliza el sistema biométrico. Este proceso requiere acciones que deben repetirse varias veces.
- **Extracción de características:** enfoque para obtener información biométrica a partir de una muestra recopilada de las características fisiológicas o de comportamiento de un usuario.
- **Precisión: la** característica más importante de los sistemas biométricos. Es qué tan correctas serán las lecturas generales.

- **Tasa de rendimiento:** la tasa a la que el sistema biométrico podrá escanear las características y completar el análisis para permitir o denegar el acceso. La velocidad aceptable es de 6 a 10 sujetos por minuto. Un solo usuario debería poder completar el proceso en 5 a 10 segundos.
- **Aceptabilidad:** describe la probabilidad de que los usuarios acepten y sigan el sistema.
- **Tasa de falso rechazo (FRR):** una medida de usuarios válidos que serán rechazados falsamente por el sistema. Esto se denomina error de tipo I.
- **Tasa de aceptación falsa (FAR):** una medida del porcentaje de usuarios inválidos que serán aceptados falsamente por el sistema. Esto se denomina error de tipo II. Los errores de tipo II son más peligrosos que los de tipo I.
- **Tasa de error de cruce (CER):** el punto en el que FRR es igual a FAR. Expresada como porcentaje, esta es la métrica más importante.

Al analizar sistemas biométricos, los profesionales de la seguridad a menudo se refieren a un gráfico Zephyr que ilustra las fortalezas y debilidades comparativas de los sistemas biométricos. Sin embargo, también debe considerar qué tan efectivo es cada sistema biométrico y su nivel de aceptación por parte del usuario. La siguiente es una lista de los métodos biométricos más populares clasificados por efectividad, siendo el más efectivo el primero:

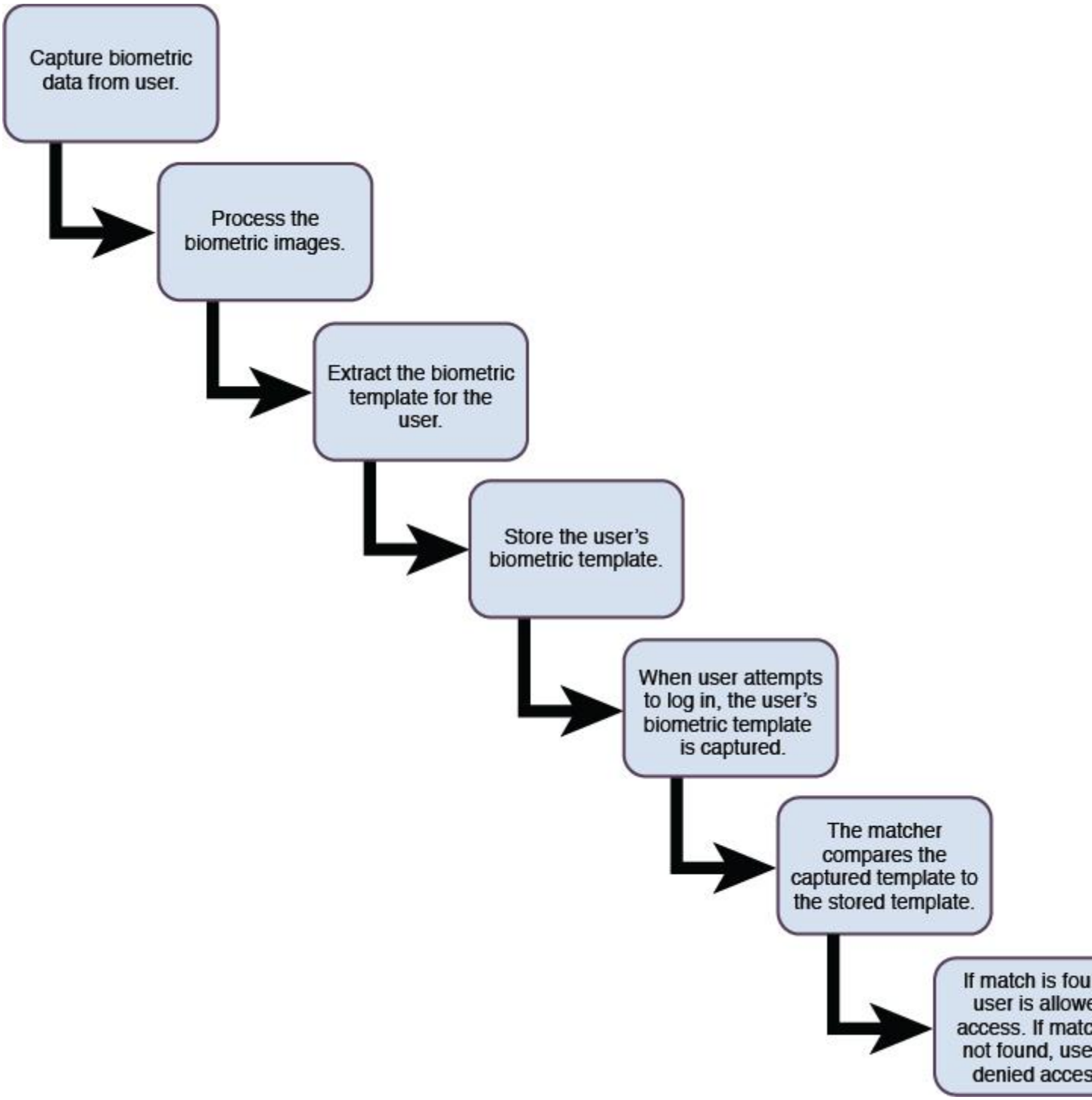
1. Escaneo de iris
2. Escaneo de retina
3. Huella dactilar
4. Impresión de mano
5. Geometría de la mano
6. Patrón de voz
7. Patrón de pulsaciones de teclas
8. Dinámica de la firma

La siguiente es una lista de los métodos biométricos más populares clasificados según la aceptación del usuario, y los métodos que los usuarios clasifican como más populares son los primeros:

1. Patrón de voz
2. Patrón de pulsaciones de teclas
3. Dinámica de la firma
4. Geometría de la mano
5. Impresión de mano
6. Huella dactilar
7. Escaneo de iris
8. Escaneo de retina

Al considerar FAR, FRR y CER, los valores más pequeños son mejores. Los errores FAR son más peligrosos que los errores FRR. Los profesionales de seguridad pueden utilizar el CER para análisis comparativos cuando ayuden a su organización a decidir qué sistema implementar. Por ejemplo, los sistemas de impresión de voz suelen tener CER más altos que los escaneos de iris, la geometría de la mano o las huellas dactilares.

La Figura 5-1 muestra el proceso de autenticación y registro biométrico.



Los pasos del proceso de autenticación y registro biométrico son los siguientes (de arriba a abajo): capturar datos biométricos del usuario, procesar las imágenes biométricas, extraer la plantilla biométrica para el usuario, almacenar la plantilla biométrica del usuario, cuando el usuario

intenta iniciar sesión , se captura la plantilla biométrica del usuario, el comparador compara la plantilla capturada con la plantilla almacenada y, si se encuentra una coincidencia, se permite el acceso del usuario. Si no se encuentra una coincidencia, se le deniega el acceso al usuario. Los pasos están conectados mediante flechas hacia abajo.

Figura 5-1 Proceso de autenticación y registro biométrico

Factores de ubicación

La autenticación del factor de ubicación proporciona un medio para autenticar al usuario en función de la ubicación desde la que se está autenticando. Esto podría incluir la computadora o el dispositivo que la persona está usando o su ubicación geográfica basada en las coordenadas GPS. El atractivo principal de este tipo de autenticación es que limita al usuario a iniciar sesión solo desde esas ubicaciones determinadas. Esto es particularmente útil en entornos de fabricación grandes para los usuarios que solo deben iniciar sesión en ciertos terminales de la instalación.

La geovalla es un ejemplo del uso de factores de ubicación. Con geo-cercas, los dispositivos solo funcionan correctamente dentro de los límites de geo-cercas. Si un dispositivo entra o sale del área geo-cercada, se genera una alerta y se envía al operador.

Factores de tiempo

La autenticación de factor de tiempo autentica a un usuario en función de la hora y / o la fecha en que el usuario se está autenticando. Por ejemplo, si ciertos usuarios trabajan solo en un horario establecido, puede configurar sus cuentas para que solo les permitan iniciar sesión durante las horas de trabajo establecidas. Sin embargo, tenga en cuenta que tal limitación podría causar problemas administrativos si se permiten horas extras. Algunas organizaciones implementan esto de manera efectiva al rellenar las horas permitidas con una o dos horas de margen para las horas de inicio y finalización. Las tarjetas de crédito utilizan esta función de forma eficaz para proteger a sus clientes. Si las transacciones se

realizan en un período corto de tiempo desde ubicaciones geográficamente dispersas, las tarjetas de crédito a menudo bloquearán la segunda transacción.

Autenticación de factor único versus autenticación de factor múltiple

La autenticación generalmente asegura que un usuario proporcione al menos un factor de las cinco categorías, lo que se conoce como autenticación de factor único. Un ejemplo de esto sería proporcionar un nombre de usuario y una contraseña al iniciar sesión. La autenticación de dos factores (2FA) garantiza que el usuario proporcione dos de los cinco factores. Un ejemplo de autenticación de dos factores sería proporcionar un nombre de usuario, contraseña y tarjeta inteligente al iniciar sesión. La autenticación de tres factores garantiza que un usuario proporcione tres factores. Un ejemplo de autenticación de tres factores sería proporcionar un nombre de usuario, contraseña, tarjeta inteligente y huella digital al iniciar sesión. Para que la autenticación se considere autenticación sólida, un usuario debe proporcionar factores de al menos dos categorías diferentes. (Tenga en cuenta que el nombre de usuario es el factor de identificación, no un factor de autenticación).

El término *autenticación multifactor* se usa a menudo cuando se usa más de un factor de autenticación. Por lo tanto, la autenticación de dos o tres factores puede denominarse autenticación de múltiples factores.

Debe comprender que proporcionar múltiples factores de autenticación de la misma categoría todavía se considera autenticación de factor único. Por ejemplo, si un usuario proporciona un nombre de usuario, una contraseña y el apellido de soltera de la madre del usuario, se utiliza la autenticación de factor único. En este ejemplo, el usuario solo proporciona factores que son algo que una persona conoce.

Autenticación de dispositivos

La autenticación de dispositivo, también conocida como autenticación de punto final, es una forma de autenticación que se basa en la identidad del

dispositivo como parte del proceso de autenticación. Con la autenticación del dispositivo, la identidad del dispositivo desde el que un usuario inicia sesión se incluye como parte del proceso de autenticación, lo que proporciona una autenticación de dos factores utilizando el dispositivo y las credenciales del usuario. Si el usuario luego intenta iniciar sesión desde un dispositivo diferente, el sistema de autenticación reconoce que se está utilizando un nuevo dispositivo y le pide al usuario que proporcione información de verificación de autenticación adicional, generalmente una respuesta a una pregunta de seguridad. Por lo general, al usuario se le da la opción de incluir este dispositivo en la autenticación (si el dispositivo es undispositivo) o no (si el dispositivo es un dispositivo público). De esta manera, el dispositivo en sí mismo se convierte en un token de seguridad y, como tal, se convierte en algo que tiene un factor de autenticación.

Los profesionales de la seguridad no deben confundir la autenticación del dispositivo con un sistema que utiliza un dispositivo móvil o correo electrónico conocidos para proporcionar una contraseña única o un PIN necesario para la autenticación. Cuando un sistema transmite la contraseña de un solo uso o el PIN que debe usarse como parte de la autenticación a un dispositivo móvil o por correo electrónico, este es solo otro factor de autenticación, no la autenticación del dispositivo. Con este sistema, el usuario registra su número de dispositivo móvil o dirección de correo electrónico con el sistema de autenticación. Cuando el usuario inicia sesión, generalmente proporciona dos factores de autenticación. Una vez que se completa la autenticación de los factores iniciales, la contraseña o PIN de un solo uso se transmite al dispositivo o correo electrónico conocido, que el usuario debe ingresar como parte de una segunda interfaz de autenticación.

Implementación de identificación y autenticación

La identificación y autenticación son pasos necesarios para proporcionar autorización. La autorización es el punto después de la identificación y autenticación en el que se otorgan a un usuario los derechos y permisos sobre los recursos. Las siguientes secciones cubren componentes importantes en la autorización: separación de tareas, privilegio mínimo / necesidad de saber, predeterminado a sin acceso, servicios de directorio, inicio de sesión único (incluidos Kerberos, SESAME, administración de identidad federada y dominios de seguridad), sesión gestión, registro y prueba de identidad, sistemas de gestión de credenciales y rendición de cuentas.

Separación de tareas

Separation of duties is an important concept to keep in mind when designing an organization's authentication and authorization policies. Separation of duties prevents fraud by distributing tasks and their associated rights and privileges between more than one user. This helps deter fraud and collusion because any fraudulent act can occur only if there is collusion. A good example of separation of duties is authorizing one person to manage backup procedures and another to manage restore procedures.

La separación de funciones está asociada con controles duales y conocimiento dividido. Con controles duales, dos o más usuarios están autorizados y requeridos para realizar ciertas funciones. Por ejemplo, un establecimiento minorista puede requerir que dos gerentes abran la caja fuerte. El conocimiento dividido garantiza que ningún usuario tenga toda la información para realizar una tarea en particular. Un ejemplo de control dividido es que los militares requieren que dos individuos ingresen cada uno en una combinación única para autorizar el disparo de misiles.

Privilegio mínimo / Necesidad de saber

El principio de privilegio mínimo requiere que a un usuario o proceso se le otorgue solo el privilegio de acceso mínimo necesario para realizar una

tarea en particular. Su objetivo principal es garantizar que los usuarios solo tengan acceso a los recursos que necesitan y estén autorizados para realizar solo las tareas que necesitan realizar. Para implementar correctamente el principio de privilegio mínimo, las organizaciones deben identificar los trabajos de todos los usuarios y restringir a los usuarios solo a los privilegios identificados.

El principio de necesidad de saber está estrechamente asociado con el concepto de privilegio mínimo. Aunque el privilegio mínimo busca reducir el acceso al mínimo, el principio de necesidad de saber realmente define cuáles son los mínimos para cada trabajo o función empresarial. Los privilegios excesivos se convierten en un problema cuando un usuario tiene más derechos, privilegios y permisos de los que necesita para hacer su trabajo. Los privilegios excesivos son difíciles de controlar en entornos grandes.

Una implementación común de los principios de privilegio mínimo y necesidad de conocer es cuando un administrador del sistema recibe tanto una cuenta de nivel administrativo como una cuenta de usuario normal. En la mayoría de las funciones diarias, el administrador debe usar su cuenta de usuario normal. Cuando el administrador del sistema necesita realizar tareas de nivel administrativo, debe usar la cuenta de nivel administrativo. Si el administrador usa su cuenta de nivel administrativo mientras realiza tareas de rutina, corre el riesgo de comprometer la seguridad del sistema y la responsabilidad del usuario.

Las reglas organizativas que apoyan el principio de privilegio mínimo son las siguientes:

- Mantenga el número de cuentas administrativas al mínimo.
- Los administradores deben utilizar cuentas de usuario normales al realizar operaciones de rutina.
- Los permisos sobre las herramientas que probablemente usen los atacantes deben ser lo más restrictivos posible.

Para respaldar más fácilmente los principios de privilegio mínimo y necesidad de saber, los usuarios deben dividirse en grupos para facilitar el confinamiento de la información a un solo grupo o área. Este proceso se conoce como compartimentación.

Predeterminado a Sin acceso

Durante el proceso de autorización, debe configurar los mecanismos de control de acceso de una organización para que el nivel predeterminado de seguridad sea el predeterminado *sin acceso* . Esto significa que si no se ha permitido nada específicamente para un usuario o grupo, el usuario o grupo no podrá acceder al recurso. El mejor enfoque de seguridad es comenzar sin acceso y agregar derechos según la necesidad del usuario de saber y el mínimo privilegio necesario para realizar sus tareas diarias.

Directorio de Servicios

Un servicio de directorio es una base de datos diseñada para centralizar la gestión de datos con respecto a los sujetos y objetos de la red. Un directorio típico contiene una jerarquía que incluye usuarios, grupos, sistemas, servidores, estaciones de trabajo cliente, etc. Debido a que el servicio de directorio contiene datos sobre usuarios y otras entidades de la red, puede ser utilizado por muchas aplicaciones que requieren acceso a esa información.

Los estándares de servicio de directorio más comunes son

- X.500
- Protocolo ligero de acceso a directorios (LDAP)
- X.400
- Servicios de dominio de Active Directory (AD DS)

X.500 utiliza el Protocolo de acceso a directorios (DAP). En X.500, el nombre distinguido (DN) proporciona la ruta completa en la base de datos X.500 donde se encuentra la entrada. El nombre distinguido relativo (RDN) en X.500 es el nombre de una entrada sin la ruta completa.

Basado en DAP de X.500, LDAP es más simple que X.500. LDAP admite DN y RDN, pero incluye más atributos como el nombre común (CN), el componente de dominio (DC) y los atributos de la unidad organizativa (OU). Usando una arquitectura cliente / servidor, LDAP usa el puerto TCP 389 para comunicarse. Si se necesita seguridad avanzada, LDAP sobre SSL se comunica a través del puerto TCP 636.

X.400 es principalmente para transferencia y almacenamiento de mensajes. Utiliza elementos para crear una serie de pares de nombre / valor separados por punto y coma. X.400 ha sido reemplazado gradualmente por implementaciones de Protocolo simple de transferencia de correo (SMTP).

La implementación de Microsoft de LDAP es Active Directory Domain Services (AD DS), que almacena y organiza los datos del directorio en árboles y bosques. También gestiona los procesos de inicio de sesión y la autenticación entre usuarios y dominios y permite a los administradores agrupar de forma lógica a los usuarios y dispositivos en unidades organizativas.

Inicio de sesión único

En un entorno de inicio de sesión único (SSO), un usuario ingresa sus credenciales de inicio de sesión una vez y puede acceder a todos los recursos de la red. El Open Group Security Forum ha definido muchos objetivos para un sistema SSO. Algunos de los objetivos de la interfaz de inicio de sesión de usuario y la gestión de cuentas de usuario son los siguientes:

- La interfaz debe ser independiente del tipo de información de autenticación manejada.
- Se debe admitir la creación, eliminación y modificación de cuentas de usuario.
- Se debe proporcionar soporte para que un usuario establezca un perfil de usuario predeterminado.

- Las cuentas deben ser independientes de cualquier plataforma o sistema operativo.

Nota

Para obtener más información sobre el estándar de inicio de sesión único de Open Group, debe acceder al sitio web en www.opengroup.org/security/sso_scope.htm .

SSO ofrece muchas ventajas y desventajas cuando se implementa.

Las ventajas de un sistema SSO incluyen

- Los usuarios pueden utilizar contraseñas más seguras.
- Se simplifica la administración de usuarios y contraseñas.
- El acceso a los recursos es mucho más rápido.
- El inicio de sesión de usuario es más eficiente.
- Los usuarios solo necesitan recordar las credenciales de inicio de sesión para un solo sistema.

Las desventajas de un sistema SSO incluyen

- Una vez que un usuario obtiene acceso al sistema a través del inicio de sesión SSO inicial, el usuario puede acceder a todos los recursos a los que tiene acceso. Aunque esto también es una ventaja para el usuario (solo se necesita un inicio de sesión), también se considera una desventaja porque solo un inicio de sesión puede comprometer todos los sistemas que participan en la red SSO.
- Si las credenciales de un usuario se ven comprometidas, los atacantes tendrán acceso a todos los recursos a los que tiene acceso el usuario.

Aunque la discusión sobre SSO hasta ahora se ha centrado principalmente en cómo se usa para redes y dominios, SSO también se puede implementar en sistemas basados en web. La gestión de acceso empresarial (EAM) proporciona gestión de control de acceso para sistemas empresariales basados en web. Sus funciones incluyen la acomodación de una variedad de métodos de autenticación y control de acceso basado en roles.

SSO se puede implementar en Kerberos, SESAME y entornos de administración de identidad federada. Luego, se pueden establecer dominios de seguridad para asignar derechos de SSO a los recursos.

Kerberos

Kerberos es un protocolo de autenticación que utiliza un modelo cliente / servidor desarrollado por Project Athena del MIT. Es el modelo de autenticación predeterminado en las ediciones recientes de Windows Server y también se usa en los sistemas operativos Apple, Oracle y Linux.Kerberos es un sistema SSO que utiliza criptografía de clave simétrica. Kerberos proporciona confidencialidad e integridad.

Kerberos asume que la mensajería, el cableado y los equipos cliente no son seguros y son de fácil acceso. En un intercambio de Kerberos que involucra un mensaje con un autenticador, el autenticador contiene el ID del cliente y una marca de tiempo. Debido a que un vale de Kerberos es válido durante un tiempo determinado, la marca de tiempo garantiza la validez de la solicitud.

En un entorno Kerberos, el Centro de distribución de claves (KDC) es el repositorio de todas las claves secretas de usuario y servicio. El cliente envía una solicitud al servidor de autenticación (AS), que puede ser o no el KDC. El AS envía las credenciales del cliente al KDC. El KDC autentica a los clientes ante otras entidades de una red y facilita la comunicación mediante claves de sesión. El KDC proporciona seguridad a los clientes o directores, que son usuarios, servicios de red y software. Cada director

debe tener una cuenta en el KDC. El KDC emite un ticket de concesión de tickets (TGT) al director. El principal enviará el TGT al servicio de concesión de boletos (TGS) cuando el principal necesite conectarse a otra entidad. El TGS luego transmite un ticket y claves de sesión al principal.

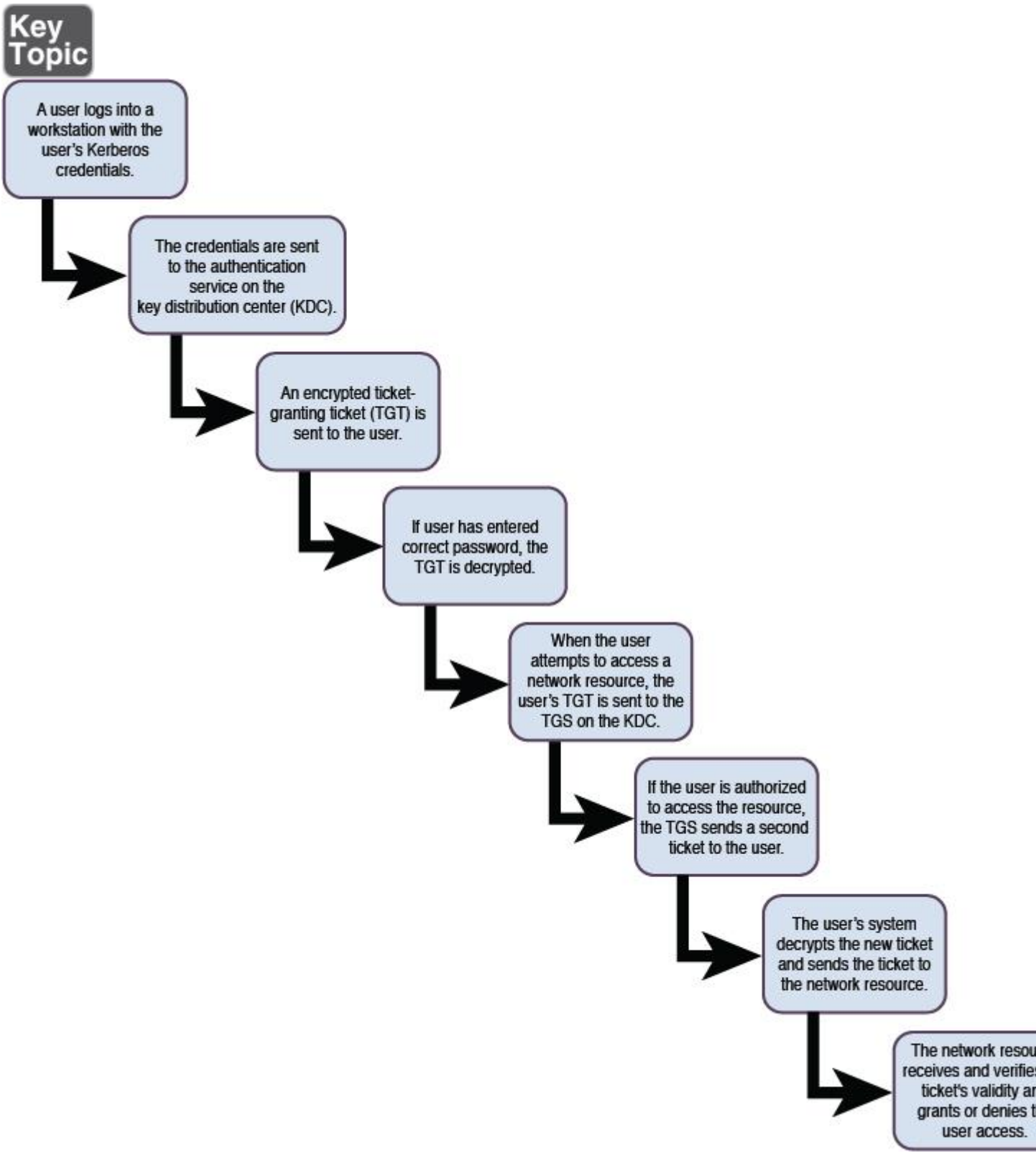
Algunas de las ventajas de implementar Kerberos incluyen las siguientes:

- Las contraseñas de usuario NO necesitan enviarse a través de la red.
- Tanto el cliente como el servidor se autentican entre sí.
- Los tickets que pasan entre el servidor y el cliente tienen una marca de tiempo e incluyen información de por vida.
- El protocolo Kerberos utiliza estándares abiertos de Internet y no se limita a códigos de propiedad o mecanismos de autenticación.

Algunas desventajas de implementar Kerberos incluyen las siguientes:

- Se requiere redundancia de KDC si se requiere tolerancia a fallas. El KDC es un único punto de falla.
- El KDC debe ser escalable para garantizar que el rendimiento del sistema no se degrade.
- Las claves de sesión en las máquinas cliente pueden verse comprometidas.
- El tráfico de Kerberos debe estar cifrado para proteger la información en la red.
- Todos los sistemas que participan en el proceso Kerberos deben tener relojes sincronizados.
- Los sistemas Kerberos son susceptibles a ataques de adivinación de contraseñas.

La Figura 5-2 muestra el proceso de emisión de tickets para Kerberos.


Key Topic
A user logs into a workstation with the user's Kerberos credentials.
The credentials are sent to the authentication service on the key distribution center (KDC).
An encrypted ticket-granting ticket (TGT) is sent to the user.
If user has entered correct password, the TGT is decrypted.
When the user attempts to access a network resource, the user's TGT is sent to the TGS on the KDC.
If the user is authorized to access the resource, the TGS sends a second ticket to the user.
The user's system decrypts the new ticket and sends the ticket to the network resource.
The network resou
receives and verifie
ticket's validity ar
grants or denies t
user access.

Los pasos del proceso de emisión de tickets de Kerberos son los siguientes (de arriba a abajo): Un usuario inicia sesión en una estación de trabajo con las credenciales de Kerberos del usuario; Las credenciales se envían al servicio de autenticación en el centro de distribución de claves (KDC); Se envía al usuario un ticket de concesión de tickets cifrado (TGT); Si el usuario ha introducido la contraseña correcta, el TGT se descifra; Cuando el usuario intenta acceder a un recurso de red, el TGT del usuario se envía al TGS en el KDC; Si el usuario está autorizado a acceder al recurso, el TGS envía un segundo ticket al usuario; El sistema del usuario descifra el nuevo ticket y lo envía al recurso de red; y El recurso de red recibe y verifica la validez del ticket y otorga o deniega el acceso del usuario. Los pasos están conectados mediante flechas hacia abajo.

Figura 5-2 Proceso de emisión de tickets de Kerberos

SÉSAMO

El proyecto Secure European System for Applications in a Multi-vendor Environment (SESAME) amplió la funcionalidad de Kerberos para corregir las debilidades de Kerberos. SESAME utiliza criptografía simétrica y asimétrica para proteger los datos intercambiados. SESAME utiliza un servidor de autenticación confiable en cada host.

SESAME utiliza certificados de atributos privilegiados (PAC) en lugar de tickets. Incorpora dos certificados: uno para autenticación y otro para definir privilegios de acceso. El servidor de autenticación de confianza se denomina Servidor de atributos privilegiados (PAS), que desempeña funciones similares a las del KDC en Kerberos. SESAME se puede integrar en un sistema Kerberos.

Gestión de identidad federada

Una identidad federada es una identidad portátil que se puede utilizar en empresas y dominios. En la gestión de identidad federada (FIM), cada organización que se une a la federación acepta hacer cumplir un conjunto común de políticas y estándares. Estas políticas y estándares definen

cómo aprovisionar y administrar la identificación, autenticación y autorización de usuarios. La gestión de identidad federada utiliza dos modelos básicos para vincular organizaciones dentro de la federación: el modelo de certificación cruzada y el modelo de terceros de confianza (o puente). A través de este modelo, se puede implementar un sistema SSO.

En el modelo de identidad federada de certificación cruzada, cada organización certifica que todas las demás organizaciones son de confianza. Esta confianza se establece cuando las organizaciones revisan los estándares de las demás. Cada organización debe verificar y certificar mediante la debida diligencia que las otras organizaciones cumplen o superan los estándares. Una desventaja de la certificación cruzada es que la cantidad de relaciones de confianza que deben administrarse puede convertirse en un problema. Además, verificar la confiabilidad de otras organizaciones puede llevar mucho tiempo y muchos recursos.

En el modelo de identidad federada de terceros de confianza (o puente), cada organización se suscribe a los estándares de un tercero. El tercero gestiona la verificación, la certificación y la diligencia debida para todas las organizaciones. Este suele ser el mejor modelo si una organización necesita establecer relaciones de administración de identidades federadas con un gran número de organizaciones.

Security Assertion Markup Language (SAML) 2.0 es un estándar SAML que intercambia datos de autenticación y autorización entre organizaciones o dominios de seguridad. Utiliza un protocolo basado en XML para pasar información sobre un principal entre una autoridad SAML y un servicio web a través de tokens de seguridad. En SAML 2.0, hay tres roles: el principal o usuario, el proveedor de identidad y el proveedor de servicios. El proveedor de servicios solicita la verificación de identidad del proveedor de identidad. SAML es muy flexible porque está basado en XML. Si una organización implementa la federación de identidad SAML empresarial, la organización puede seleccionar qué atributos de identidad compartir con otra organización.

Dominios de seguridad

Un dominio es un conjunto de recursos que está disponible para un sujeto a través de una red. Los sujetos que acceden a un dominio incluyen usuarios, procesos y aplicaciones. Un dominio de seguridad es un conjunto de recursos que sigue las mismas políticas de seguridad y está disponible para un sujeto. Los dominios generalmente se organizan en una estructura jerárquica de dominios principales y secundarios.

Nota

No confunda el término *dominio de seguridad* con dominio de protección. Aunque un dominio de seguridad generalmente abarca una red, un dominio de protección reside dentro de un solo recurso. Un *dominio de protección* es un grupo de procesos que comparte el acceso al mismo recurso.

Gestión de sesiones

La gestión de sesiones garantiza que cualquier instancia de identificación y autenticación de un recurso se gestione correctamente. Esto incluye la gestión de sesiones de escritorio y sesiones remotas.

Las sesiones de escritorio deben administrarse a través de una variedad de mecanismos. Los protectores de pantalla permiten bloquear las computadoras si se dejan inactivas durante un cierto período de tiempo. Para reactivar una computadora, el usuario debe volver a iniciar sesión. Los protectores de pantalla son un mecanismo de tiempo de espera y también se pueden usar otras funciones de tiempo de espera, como apagar o poner una computadora en hibernación después de un período determinado. Las limitaciones de sesión o inicio de sesión permiten a las organizaciones configurar cuántas sesiones simultáneas puede tener un usuario. Las limitaciones de programación permiten a las organizaciones configurar el tiempo durante el cual un usuario puede acceder a una computadora.

Las sesiones remotas generalmente incorporan algunos de los mismos mecanismos que las sesiones de escritorio. Sin embargo, las sesiones remotas no ocurren en la propia computadora. Más bien, se llevan a cabo a través de una conexión de red. Las sesiones remotas siempre deben utilizar protocolos de conexión seguros. Además, si los usuarios solo se conectarán de forma remota desde ciertas computadoras, es posible que la organización desee implementar algún tipo de acceso basado en reglas que permita solo ciertas conexiones.

Registro y prueba de identidad

Un proceso de prueba de identidad implica recopilar y verificar información sobre una persona para demostrar que la persona que tiene una cuenta válida es quien dice ser. El método más básico de prueba de identidad es proporcionar una licencia de conducir, pasaporte o alguna otra identificación emitida por el gobierno. La prueba de identidad se realiza antes de la creación de la cuenta de usuario. Una vez que se completa la prueba de identidad, se emite una credencial al usuario y se determinan y registran los factores de autenticación. A partir de ese momento, la autenticación se produce cada vez que el usuario inicia sesión con la credencial emitida.

El Instituto Nacional de Estándares y Tecnología (NIST) ha emitido documentos que brindan orientación sobre la prueba de identidad:

- Publicación FIPS 201-2, *Verificación de identidad personal (PIV) de empleados y contratistas federales* : este documento especifica la arquitectura y los requisitos técnicos para un estándar de identificación común para empleados y contratistas federales. Esta publicación incluye requisitos de identificación, seguridad y privacidad y pautas del sistema de verificación de identidad personal.
- NIST SP 800-79-2, *Pautas para la autorización de emisores de tarjetas de verificación de identidad personal (PCI) y emisores de credenciales PIV derivados (DPCI)* : este documento incluye pautas

de preparación, pautas de implementación de control de emisores y pautas de ciclo de vida de control de emisores.

Ambas publicaciones del NIST están destinadas a guiar a las agencias del gobierno federal en sus esfuerzos de prueba de identidad y también pueden ser utilizadas por organizaciones privadas para ayudar en el desarrollo de sus propios sistemas.

Sistemas de gestión de credenciales

Los usuarios a menudo deben recordar nombres de usuario, contraseñas y otra información de autenticación para una variedad de organizaciones. A menudo usan las mismas credenciales de autenticación en múltiples plataformas, lo que hace que el robo de identidad y el fraude en línea sean más fáciles de cometer. Una vez que se ha descubierto un conjunto de credenciales en un sistema en línea, los atacantes suelen utilizar el mismo conjunto de credenciales en los sistemas de otra organización para ver si pueden obtener acceso. Junto con este problema viene el problema interno de una organización para mantener diferentes credenciales para los usuarios que necesitan acceso a múltiples sistemas con diferentes sistemas de credenciales. Tenga en cuenta el uso cada vez mayor de dispositivos móviles y tendrá una receta para el desastre.

Los sistemas de gestión de credenciales permiten a las organizaciones establecer un marco de autorización y autenticación de usuarios en toda la empresa. Las organizaciones deben emplear profesionales de seguridad para diseñar, implementar y administrar sistemas seguros de administración de credenciales. Los requisitos comerciales para un sistema de gestión de credenciales deben incluir pautas de protección de la privacidad individual, soluciones de identidad automatizadas, seguridad e innovación. Algunas de las pautas de un sistema de gestión de credenciales incluyen las siguientes:

- Utilice contraseñas seguras.
- Genere automáticamente contraseñas complejas.

- Implementar el historial de contraseñas.
- Utilice mecanismos de control de acceso, incluido quién, qué, cómo y cuándo acceder.
- Implementar auditorías.
- Implemente mecanismos de copia de seguridad y restauración para la integridad de los datos.
- Implemente sistemas redundantes dentro de los sistemas de gestión de credenciales para garantizar el acceso las 24 horas del día, los 7 días de la semana, los 365 días del año.
- Implementar políticas de grupo de administración de credenciales u otros mecanismos ofrecidos por los sistemas operativos.

Cuando una organización implementa un sistema de gestión de credenciales, la separación de funciones se vuelve aún más importante porque el sistema de gestión de credenciales centralizado se puede utilizar para cometer fraude. Los profesionales de seguridad deben brindar orientación sobre cómo debe ocurrir la separación para proteger mejor a la organización y sus activos.

Responsabilidad

La rendición de cuentas es la capacidad de una organización para responsabilizar a los usuarios de las acciones que realizan. Para asegurar que los usuarios sean responsables de sus acciones, las organizaciones deben implementar auditorías y otros mecanismos de rendición de cuentas.

Para garantizar que los usuarios sean responsables de sus acciones, las organizaciones podrían implementar cualquier combinación de los siguientes componentes:

- **Fuerte identificación:** cada usuario debe tener su propia cuenta. Las cuentas de grupos o roles no se pueden rastrear hasta una sola persona.

- **Autenticación** sólida **: la autenticación** multifactor es la mejor. Como mínimo, se debe implementar la autenticación de dos factores.
- **Supervisión: las** acciones del usuario deben supervisarse, incluido el inicio de sesión, el uso de privilegios y otras acciones. Se debe advertir a los usuarios como parte de una declaración de no expectativa de privacidad que todas las acciones pueden ser monitoreadas.
- **Registros de auditoría: los registros de** auditoría deben mantenerse y almacenarse de acuerdo con las políticas de seguridad de la organización. Los administradores deben revisar estos registros periódicamente.

Si bien las organizaciones deben implementar internamente estos mecanismos de rendición de cuentas, también deben hacer que un tercero realice auditorías y pruebas periódicamente. Esto es importante porque el tercero externo puede brindar una objetividad que el personal interno a menudo no puede brindar.

Auditoría e informes

La auditoría y la generación de informes garantizan que los usuarios sean responsables de sus acciones, pero un mecanismo de auditoría solo puede informar sobre eventos que está configurado para monitorear. Debe monitorear los eventos de la red, los eventos del sistema, los eventos de la aplicación, los eventos del usuario y la actividad de pulsaciones de teclas. Tenga en cuenta que cualquier actividad de auditoría afectará el rendimiento del sistema que se supervisa. Las organizaciones deben encontrar un equilibrioentre la auditoría de eventos y actividades importantes y la garantía de que el rendimiento del dispositivo se mantiene a un nivel aceptable. Además, las organizaciones deben asegurarse de que cualquier monitoreo que se lleve a cabo cumpla con todas las leyes aplicables.

Al diseñar un mecanismo de auditoría, los profesionales de seguridad deben recordar las siguientes pautas:

- Desarrolle un plan de gestión de registros de auditoría que incluya mecanismos para controlar el tamaño del registro, los procesos de respaldo y los planes de revisión periódica.
- Asegúrese de que la capacidad de eliminar un registro de auditoría sea un control de dos personas que requiera la cooperación de al menos dos administradores. Esto asegura que un solo administrador no pueda eliminar registros que puedan contener evidencia incriminatoria.
- Supervise todas las cuentas con privilegios elevados (incluidos todos los usuarios raíz y las cuentas de nivel administrativo).
- Asegúrese de que la pista de auditoría incluya quién procesó la transacción, cuándo ocurrió la transacción (fecha y hora), dónde ocurrió la transacción (qué sistema) y si la transacción fue exitosa o no.
- Asegúrese de que la eliminación del registro y la eliminación de datos dentro de los registros no puedan ocurrir a menos que el usuario tenga los permisos de nivel administrativo adecuados.

Nota

La depuración es el acto de eliminar datos incriminatorios dentro de un registro de auditoría.

Las pistas de auditoría detectan penetraciones informáticas y revelan acciones que identifican el uso indebido. Como profesional de la seguridad, debe utilizar las pistas de auditoría para revisar los patrones de acceso a objetos individuales. Para identificar patrones anormales de comportamiento, primero debe identificar patrones normales de comportamiento. Además, debe establecer el nivel de recorte, que es una

línea de base de los errores del usuario por encima del cual se registrarán las infracciones. Por ejemplo, su organización puede optar por ignorar el primer intento de inicio de sesión no válido, sabiendo que los intentos iniciales de inicio de sesión fallidos a menudo se deben a un error del usuario. Cualquier inicio de sesión no válido después del primero se registraría porque podría ser una señal de un ataque. Un nivel de recorte común que se utiliza son tres intentos fallidos de inicio de sesión. Cualquier intento de inicio de sesión fallido por encima del límite de tres se considerará malicioso. En la mayoría de los casos,

Las pistas de auditoría disuaden a los atacantes de intentar eludir los mecanismos de protección configurados en un sistema o dispositivo. Como profesional de la seguridad, debe configurar específicamente las pistas de auditoría para rastrear los derechos o privilegios del sistema / dispositivo que se otorgan a un usuario y las adiciones, eliminaciones o modificaciones de datos.

Finalmente, se deben monitorear las pistas de auditoría y se deben configurar las notificaciones automáticas. Si nadie supervisa la pista de auditoría, los datos registrados en la pista de auditoría son inútiles. Ciertas acciones deben configurarse para activar notificaciones automáticas. Por ejemplo, es posible que desee configurar una alerta de correo electrónico para que se produzca después de una cierta cantidad de intentos de inicio de sesión no válidos porque los intentos de inicio de sesión no válidos pueden ser una señal de que se está produciendo un ataque de contraseña por fuerza bruta.

Implementación de la identidad como servicio (IDaaS)

Identity as a Service (IDaaS) proporciona un conjunto de funciones de gestión de acceso e identidad para los sistemas de destino en las instalaciones de los clientes y / o en la nube. IDaaS incluye la gobernanza y la administración de identidades (IGA), que brinda la capacidad de proporcionar identidades en poder del servicio para aplicaciones de

destino. Incluye autenticación de usuario, inicio de sesión único (SSO) y aplicación de autorización. Los servicios IDaaS se dividen en dos categorías: software de acceso web para aplicaciones basadas en la nube y servicios de gestión de identidad heredados entregados en la nube. Las aplicaciones Web IDaaS no funcionan con aplicaciones locales. La mayoría de las implementaciones de IDaaS ofrecen autenticación SSO, identidades federadas, administración remota e integración del servicio de directorio interno. IDaaS es diferente de las soluciones de administración de identidad y acceso (IAM), que se operan desde la propia red de la organización a través de un paquete de software y hardware. Las soluciones de IAM pueden utilizar Active Directory y LDAP.

Si las organizaciones consideran la implementación de IDaaS, deben preocuparse principalmente por la disponibilidad del servicio, la protección de los datos de identidad y confiar en un tercero con una función comercial crítica. También deberían preocuparse por el cumplimiento normativo. Trasladar la gestión de identidades a la nube genera una gran cantidad de preguntas para la organización con respecto a la auditoría, la garantía del cumplimiento de las regulaciones y lo que sucede si se producen divulgaciones.

Una organización debe realizar un análisis de riesgos integral antes de implementar cualquier servicio IDaaS. Después de realizar el análisis de riesgos, la organización debe determinar qué identidades deben colocarse en la solución IDaaS.

Integración de servicios de identidad de terceros

Si una organización decide implementar un servicio de identidad de terceros, incluidas las soluciones de computación en la nube, los profesionales de la seguridad deben participar en la integración de esa implementación con los servicios y recursos internos. Esta integración puede ser compleja, especialmente si la solución del proveedor no es totalmente compatible con los sistemas internos existentes. La mayoría

de los servicios de identidad de terceros proporcionan identidad en la nube, sincronización de directorios e identidad federada. Ejemplos de estos servicios incluyen el servicio de administración de acceso e identidad (IAM) de Amazon Web Services (AWS) y Oracle Identity Management.

Los servicios de identidad de terceros incluyen servicios locales, en la nube y federados. Estos tres tipos de servicios se analizan a lo largo de este capítulo.

Mecanismos de autorización

Los mecanismos de autorización son sistemas que implementa una organización para controlar a qué sistemas puede acceder un usuario o dispositivo. Los mecanismos de autorización incluyen modelos de control de acceso y políticas de control de acceso.

Permisos, derechos y privilegios

Los permisos se otorgan o deniegan a nivel de archivo, carpeta u otro objeto. Los tipos de permisos comunes incluyen lectura, escritura y control total. Los custodios o administradores de datos otorgarán permisos a los usuarios sobre un archivo o carpeta según la solicitud del propietario para hacerlo.

Los derechos permiten a los administradores asignar privilegios específicos y derechos de inicio de sesión a grupos o usuarios. Los derechos administran quién puede realizar ciertas operaciones en una computadora completa o dentro de un dominio, en lugar de un objeto particular dentro de una computadora. Si bien los permisos de usuario son otorgados por el propietario de un objeto, los derechos de usuario se asignan mediante la política de seguridad local de una computadora o una política de seguridad de dominio. Los derechos de usuario se aplican a las cuentas de usuario, mientras que los permisos se aplican a los objetos.

Los derechos incluyen la capacidad de iniciar sesión en un sistema de forma interactiva, que es un derecho de inicio de sesión, o la capacidad de realizar copias de seguridad de archivos, que se considera un privilegio. Los derechos de usuario se dividen en dos categorías: privilegios y derechos de inicio de sesión. Los privilegios son el derecho de una cuenta, como una cuenta de usuario o de grupo, para realizar varias operaciones relacionadas con el sistema en la computadora local, como apagar el sistema, cargar controladores de dispositivos o cambiar la hora del sistema. Los derechos de inicio de sesión controlan la forma en que los usuarios pueden acceder a la computadora, incluido el inicio de sesión localmente, a través de una conexión de red, como servicio o como trabajo por lotes.

Los conflictos pueden ocurrir en situaciones en las que los derechos que se requieren para administrar un sistema se superponen con los derechos de propiedad de los recursos. Cuando los derechos entran en conflicto, un privilegio anula un permiso.

Modelos de control de acceso

Un modelo de control de acceso es una descripción formal de la política de seguridad de una organización. Los modelos de control de acceso se implementan para simplificar la administración del control de acceso agrupando objetos y sujetos. Los sujetos son entidades que solicitan acceso a un objeto o datos dentro de un objeto. Los usuarios, programas y procesos son sujetos. Los objetos son entidades que contienen información o funcionalidad. Las computadoras, las bases de datos, los archivos, los programas, los directorios y los campos son objetos. Un modelo de control de acceso seguro debe garantizar que los objetos seguros no puedan fluir hacia un sujeto menos seguro.

Los modelos y conceptos de control de acceso que debe comprender son los siguientes:

- Control de acceso discrecional

- Control de acceso obligatorio
- Control de acceso basado en roles
- Control de acceso basado en reglas
- Control de acceso basado en atributos
- Control de acceso dependiente del contenido versus dependiente del contexto
- Matriz de control de acceso
- Tabla de capacidades
- ACL

Control de acceso discrecional

En el control de acceso discrecional (DAC), el propietario del objeto especifica qué sujetos pueden acceder al recurso. DAC se utiliza normalmente en situaciones dinámicas locales. El acceso se basa en la identidad, el perfil o el rol del sujeto. Se considera que el DAC es un control imprescindible.

DAC puede ser una carga administrativa porque el custodio o propietario de los datos otorga privilegios de acceso a los usuarios. Bajo DAC, los derechos de un sujeto deben terminarse cuando el sujeto deja la organización. El control de acceso basado en identidad es un subconjunto de DAC y se basa en la identidad del usuario o en la pertenencia a un grupo.

El control de acceso no discrecional es lo opuesto al DAC. En el control de acceso no discrecional, los controles de acceso los configura un administrador de seguridad u otra autoridad. La autoridad central decide qué sujetos tienen acceso a los objetos según la política de la organización. En el control de acceso no discrecional, el sistema compara la identidad del sujeto con el ACL de los objetos.

Control de acceso obligatorio

En el control de acceso obligatorio (MAC), la autorización del sujeto se basa en etiquetas de seguridad. MAC se describe a menudo como

prohibitivo porque se basa en un sistema de etiquetas de seguridad. Bajo MAC, todo lo que no está expresamente permitido está prohibido. Solo los administradores pueden cambiar la categoría de un recurso.

MAC es más seguro que DAC. DAC es más flexible y escalable que MAC. Debido a la importancia de la seguridad en MAC, se requiere etiquetado. La clasificación de datos refleja la sensibilidad de los datos. En un sistema MAC, una autorización es un privilegio del sujeto. A cada sujeto y objeto se le asigna una etiqueta de seguridad o confidencialidad. Las etiquetas de seguridad son jerárquicas. Para las organizaciones comerciales, los niveles de etiquetas de seguridadpodría ser confidencial, patentado, corporativo, sensible y público. Para las instituciones gubernamentales o militares, los niveles de las etiquetas de seguridad pueden ser de alto secreto, secreto, confidencial y sin clasificar.

En MAC, el sistema toma decisiones de acceso cuando compara el nivel de autorización del sujeto con la etiqueta de seguridad del objeto.

Control de acceso basado en roles

En el control de acceso basado en roles (RBAC), a cada sujeto se le asigna uno o más roles. Los roles son jerárquicos. El control de acceso se define en función de los roles. RBAC se puede utilizar para hacer cumplir fácilmente los privilegios mínimos para los sujetos. Un ejemplo de RBAC es la implementación de una política de control de acceso para los cajeros bancarios y otra política para los oficiales de crédito.

RBAC no es tan seguro como los modelos de control de acceso mencionados anteriormente porque la seguridad se basa en roles. El RBAC generalmente tiene un costo de implementación mucho menor que los otros modelos y es popular en aplicaciones comerciales. Es una excelente opción para organizaciones con alta rotación de empleados. RBAC puede reemplazar eficazmente DAC y MAC porque le permite especificar y hacer cumplir las políticas de seguridad empresarial de una manera que se corresponda con la estructura de la organización.

RBAC se gestiona de cuatro formas. En no RBAC, no se utilizan roles. En RBAC limitado, los usuarios se asignan a roles de aplicación únicos, pero algunas aplicaciones no usan RBAC y requieren acceso basado en identidad. En RBAC híbrido, cada usuario se asigna a un solo rol, lo que les da acceso a múltiples sistemas, pero cada usuario puede asignarse a otros roles que tienen acceso a sistemas únicos. En el RBAC completo, los usuarios se asignan a un solo rol según lo definido por la política de seguridad de la organización, y el acceso a los sistemas se administra a través de los roles organizacionales.

Control de acceso basado en reglas

El control de acceso basado en reglas facilita cambios frecuentes en los permisos de datos y se define en RFC 2828. Con este método, una política de seguridad se basa en reglas globales impuestas para todos los usuarios. Los perfiles se utilizan para controlar el acceso. Muchos enrutadores y firewalls utilizan este tipo de control de acceso y definen qué tipos de paquetes están permitidos en una red. Las reglas se pueden escribir permitiendo o denegando el acceso según el tipo de paquete, el número de puerto utilizado, la dirección MAC y otros parámetros.

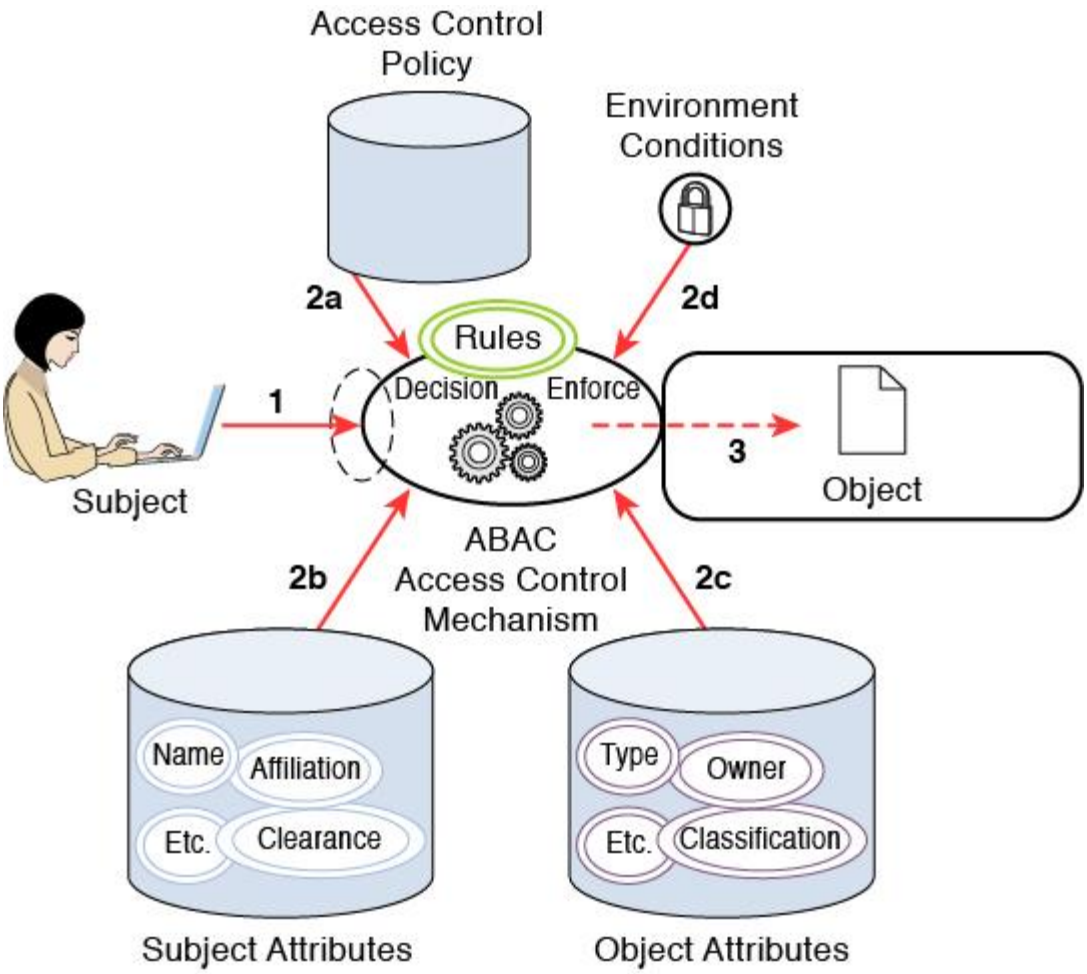
Control de acceso basado en atributos

El control de acceso basado en atributos (ABAC) otorga o niega las solicitudes de los usuarios en función de atributos arbitrarios del usuario y atributos arbitrarios del objeto, y las condiciones ambientales que pueden ser reconocidas globalmente. NIST SP 800-162 se publicó para definir y aclarar ABAC.

De acuerdo con NIST SP 800-162, ABAC es un método de control de acceso en el que las solicitudes de sujetos para realizar operaciones en objetos se otorgan o niegan en función de los atributos asignados del sujeto, los atributos asignados del objeto, las condiciones ambientales y un conjunto de políticas que son especificado en términos de esos atributos y condiciones. Una operación es la ejecución de una función a petición de un sujeto sobre un objeto. Las operaciones incluyen leer,

escribir, editar, eliminar, copiar, ejecutar y modificar. Una política es la representación de reglas o relaciones que permite determinar si se debe permitir un acceso solicitado, dados los valores de los atributos del sujeto, objeto y posiblemente las condiciones ambientales. Las condiciones ambientales son el contexto operacional o situacional en el que ocurren las solicitudes de acceso. Las condiciones ambientales son características ambientales detectables. Las características del entorno son independientes del sujeto u objeto y pueden incluir la hora actual, el día de la semana, la ubicación de un usuario o el nivel de amenaza actual.

La Figura 5-3 muestra un escenario ABAC básico según NIST SP 800-162.



1. Subject requests access to object.
2. Access control mechanism evaluates
    a) Rules
    b) Subject attributes
    c) Object attributes
    d) Environment conditions to compute a decision
3. Subject is given access to object if authorized.

¿¿La A?? B ?? A ?? El mecanismo de control C en el centro muestra una forma ovalada etiquetada como "Reglas" que representa la decisión y el cumplimiento con la imagen prediseñada de la configuración. Una flecha hacia la derecha del usuario con una computadora portátil con la etiqueta "1" apunta a las reglas. Una flecha hacia abajo de un cilindro vacío que representa una política de control de acceso etiquetada como "2a" apunta a las reglas. Una flecha hacia arriba de un contenedor cilíndrico

que consta de nombre, afiliación, autorización, etc., que representa los atributos del sujeto etiquetados como "2b" apunta a las reglas. La flecha hacia arriba de un contenedor cilíndrico que consta de tipo, propietario, clasificación, etc., que representa los atributos del objeto etiquetados "2c" apunta a las reglas. Una flecha punteada hacia la derecha desde las reglas apunta a la carpeta que representa un objeto con la etiqueta "3". Una flecha hacia abajo de un candado encerrado en un círculo representa "2d". El texto debajo de la figura dice: 1. El sujeto solicita acceso al objeto. 2. El mecanismo de control de acceso evalúa a) Reglas b) Atributos del sujeto c) Atributos del objeto d) Condiciones ambientales para calcular una decisión 3. El sujeto tiene acceso al objeto si está autorizado.

Figura 5-3 Escenario ABAC básico NIST SP 800-162

Como se especifica en NIST SP 800-162, hay características o atributos de un sujeto como el nombre, la fecha de nacimiento, la dirección del hogar, el registro de capacitación y la función laboral que pueden, ya sea individualmente o cuando se combinan, comprender una identidad única que distingue que persona de todos los demás. Estas características se denominan a menudo atributos del sujeto.

Al igual que los sujetos, cada objeto tiene un conjunto de atributos que ayudan a describirlo e identificarlo. Estos rasgos se denominan atributos de objeto y, a veces, se denominan atributos de recursos. Los atributos de objeto suelen estar vinculados a sus objetos mediante referencia, incrustándolos dentro del objeto o mediante algún otro medio de asociación asegurada, como la vinculación criptográfica.

Las ACL y RBAC son de alguna manera casos especiales de ABAC en términos de los atributos utilizados. Las ACL funcionan con el atributo de "identidad". RBAC trabaja en el atributo de "rol". La diferencia clave con ABAC es el concepto de políticas que expresan un complejo conjunto de reglas booleanas que pueden evaluar muchos atributos diferentes. Si bien es posible lograr los objetivos de ABAC utilizando ACL o RBAC, demostrar el cumplimiento de los requisitos de control de acceso es difícil y costoso

debido al nivel de abstracción requerido entre los requisitos de control de acceso y el modelo ACL o RBAC. Otro problema con los modelos ACL o RBAC es que si se cambia el requisito de control de acceso, puede ser difícil identificar todos los lugares donde se debe actualizar la implementación de ACL o RBAC.

ABAC se basa en la asignación de atributos a sujetos y objetos, y en el desarrollo de políticas que contienen las reglas de acceso. A cada objeto dentro del sistema se le deben asignar atributos de objeto específicos que caracterizan al objeto. Algunos atributos pertenecen a la instancia completa de un objeto, como el propietario. Es posible que otros atributos solo se apliquen a partes del objeto.

A cada sujeto que utiliza el sistema se le deben asignar atributos específicos. Cada objeto dentro del sistema debe tener al menos una política que defina las reglas de acceso para los sujetos, las operaciones y las condiciones ambientales permitidas para el objeto. Esta política normalmente se deriva de reglas documentadas o de procedimiento que describen los procesos comerciales y las acciones permitidas dentro de la organización. Las reglas que unen los atributos de sujeto y objeto especifican indirectamente privilegios (es decir, qué sujetos pueden realizar qué operaciones en qué objetos). Las reglas de operación permitidas se pueden expresar a través de muchas formas de lenguaje computacional, como

- Una combinación booleana de atributos y condiciones que satisfacen la autorización para una operación específica.
- Un conjunto de relaciones que asocian atributos de sujeto y objeto y operaciones permitidas.

Una vez que se establecen los atributos del objeto, los atributos del sujeto y las políticas, los objetos se pueden proteger mediante ABAC. Los mecanismos de control de acceso median el acceso a los objetos al limitar el acceso a las operaciones permitidas por los sujetos permitidos. El mecanismo de control de acceso ensambla la política, los atributos del

sujeto y los atributos del objeto, luego procesa y aplica una decisión basada en la lógica proporcionada en la política. Los mecanismos de control de acceso deben poder gestionar el proceso necesario para tomar y hacer cumplir la decisión, incluida la determinación de qué política recuperar, qué atributos recuperar en qué orden y dónde recuperar atributos. El mecanismo de control de acceso debe entonces realizar el cálculo necesario para tomar una decisión.

Las políticas que se pueden implementar en un modelo ABAC están limitadas solo al grado impuesto por el lenguaje computacional y la riqueza de los atributos disponibles. Esta flexibilidad permite que la mayor amplitud de sujetos acceda a la mayor amplitud de objetos sin tener que especificar las relaciones individuales entre cada sujeto y cada objeto.

Si bien ABAC permite compartir información, el conjunto de componentes necesarios para implementar ABAC se vuelve más complejo cuando se implementa en una empresa. A nivel empresarial, el aumento de la escala requiere capacidades de gestión complejas y, a veces, establecidas de forma independiente, necesarias para garantizar el uso compartido y el uso coherente de políticas y atributos y la distribución controlada y el empleo de mecanismos de control de acceso en toda la empresa.

Dependiente del contenido versus dependiente del contexto

El control de acceso dependiente del contenido toma decisiones de acceso basadas en los datos contenidos dentro del objeto. Con este control de acceso, los datos que ve un usuario pueden cambiar según la política y las reglas de acceso que se apliquen.

El control de acceso dependiente del contexto se basa en atributos del sujeto u objeto o características ambientales. Estas características pueden incluir la ubicación o la hora del día. Un ejemplo de esto es si los administradores implementan una política de seguridad que garantiza

que un usuario solo inicie sesión desde una estación de trabajo en particular durante ciertas horas del día.

Los expertos en seguridad consideran una interfaz de usuario restringida como otro método de control de acceso. Un ejemplo de una interfaz de usuario restringida es un shell, que es una interfaz de software para un sistema operativo que implementa el control de acceso al limitar los comandos del sistema que están disponibles. Otro ejemplo son las vistas de la base de datos que se filtran según los criterios del usuario o del sistema. Las interfaces de usuario restringidas pueden depender del contenido o del contexto en función de cómo el administrador restringe la interfaz.

Matriz de control de acceso

Una matriz de control de acceso es una tabla que consta de una lista de sujetos, una lista de objetos y una lista de las acciones que un sujeto puede realizar sobre cada objeto. Las filas en ella matriz son los sujetos y las columnas de la matriz son los objetos. Las implementaciones comunes de una matriz de control de acceso incluyen una tabla de capacidades y una ACL.

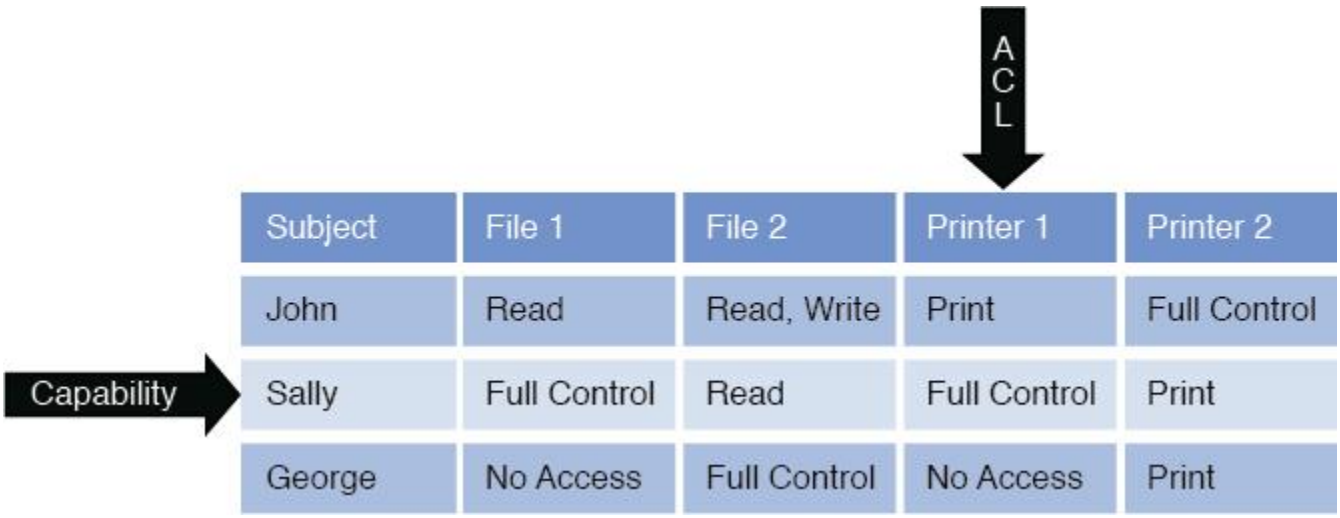
Tabla de capacidades

Una capacidad corresponde a la fila de un sujeto de una matriz de control de acceso. Una tabla de capacidades enumera los derechos de acceso que un sujeto en particular tiene a los objetos. Una tabla de capacidades trata sobre el tema.

ACL

Una ACL corresponde a la columna de un objeto de una matriz de control de acceso. Una ACL enumera todos los derechos de acceso que los sujetos tienen a un objeto en particular. Una LCA trata sobre el objeto.

La Figura 5-4 muestra una matriz de control de acceso y cómo una capacidad y ACL son parte de ella.



Se muestran cinco columnas y tres filas. Los encabezados de fila dicen: Asunto, Archivo 1, Archivo 2, Impresora 1 e Impresora 2. La fila 1 dice: Juan, Lectura, Lectura, Escritura, Impresión y Control total. La fila 2 dice: Sally, Control total, Leer, Control total e Imprimir. La fila 3 dice: George, Sin acceso, Control total, Sin acceso e Imprimir. Una flecha hacia la derecha que dice "Capacidad" apunta a la fila 2 y una flecha hacia abajo que dice "ACL" apunta a la columna 4.

Figura 5-4 Matriz de control de acceso

Políticas de control de acceso

Una política de control de acceso define el método para identificar y autenticar a los usuarios y el nivel de acceso que se les otorga. Las organizaciones deben implementar políticas de control de acceso para garantizar que las decisiones de control de acceso de los usuarios se basen en pautas formales. Si no se adopta una política de control de acceso, las organizaciones tendrán problemas para asignar, gestionar y administrar la gestión de acceso.

Ciclo de vida de aprovisionamiento

Las organizaciones deben crear un proceso formal para crear, cambiar y eliminar usuarios, que es el ciclo de vida del aprovisionamiento. Este proceso incluye la aprobación de usuarios, la creación de usuarios, los estándares de creación de usuarios y la autorización. Los usuarios deben firmar una declaración escrita que explique las condiciones de acceso, incluidas las responsabilidades del usuario. Por último, se deben documentar los procedimientos de modificación y eliminación de acceso.

Aprovisionamiento

Las políticas de aprovisionamiento de usuarios deben integrarse como parte de la gestión de recursos humanos. Las políticas de recursos humanos deben incluir procedimientos mediante los cuales el departamento de recursos humanos solicite formalmente la creación o eliminación de una cuenta de usuario cuando se contrata o termina personal nuevo.

Gestión de identidades y cuentas

La administración de identidades y cuentas es vital para cualquier proceso de autenticación. Como profesional de la seguridad, debe asegurarse de que su organización tenga un procedimiento formal para controlar la creación y asignación de credenciales o identidades de acceso. Si se permite la creación de cuentas no válidas y no se deshabilitan, se producirán violaciones de seguridad. La mayoría de las organizaciones implementan un método para revisar el proceso de identificación y autenticación para asegurarse de que las cuentas de los usuarios estén actualizadas. Las preguntas que probablemente ayudarán en el proceso incluyen

- ¿Se mantiene y aprueba una lista actualizada de usuarios, dispositivos y servicios autorizados y su acceso?
- ¿Se cambian las contraseñas al menos cada 90 días o antes si es necesario?
- ¿Se desactivan las cuentas de usuario, dispositivo y servicio inactivos después de un período de tiempo específico?

Cualquier procedimiento de administración de identidad debe incluir procesos para crear (aprovisionamiento), cambiar y monitorear (revisar) y eliminar usuarios, dispositivos y servicios del sistema de control de acceso (revocación). Esto se conoce como ciclo de vida de aprovisionamiento. Al establecer inicialmente una cuenta de usuario, se debe solicitar a los nuevos usuarios que proporcionen una identificación con foto válida y deben firmar una declaración sobre la confidencialidad de la contraseña. Para las cuentas de dispositivo y servicio, el propietario del dispositivo o servicio debe solicitar la creación de la cuenta. Las cuentas de usuario, dispositivo y servicio deben ser únicas. Deben existir políticas que estandaricen la estructura de las cuentas de usuario, dispositivo y servicio. Por ejemplo, todas las cuentas de usuario deben ser *firstname* . *apellido*o alguna otra estructura. Esto asegura que los usuarios dentro de una organización podrán determinar la identificación de un nuevo usuario, principalmente con fines de comunicación. También deben adoptarse convenciones de nomenclatura de dispositivos y servicios.

Después de la creación, las cuentas deben supervisarse para asegurarse de que permanezcan activas. Las cuentas inactivas deben desactivarse automáticamente después de un cierto período de inactividad según los requisitos comerciales. Además, cualquier política de terminación debe incluir procedimientos formales para garantizar que todas las cuentas se deshabiliten o eliminen. Los elementos de una gestión de cuentas adecuada incluyen los siguientes:

- Establezca un proceso formal para establecer, emitir y cerrar cuentas.
- Revise periódicamente las cuentas.
- Implemente un proceso para rastrear la autorización de acceso.
- Revisar periódicamente al personal en puestos delicados.
- Verifique periódicamente la legitimidad de las cuentas.

Las revisiones de cuentas son una parte vital de la administración de cuentas. Las cuentas deben revisarse para verificar su conformidad con el principio de privilegio mínimo. (El principio de privilegios mínimos se

explica más adelante en este capítulo). Las revisiones de cuentas se pueden realizar en toda la empresa, en todo el sistema o aplicación por aplicación. El tamaño de la organización afectará en gran medida cuál de estos métodos utilizar. Como parte de las revisiones de cuentas, las organizaciones deben determinar si todas las cuentas están activas.

Revisión de acceso a cuentas de usuario y sistema

La revisión de la cuenta debe realizarse periódicamente para determinar que todas las cuentas que se han creado todavía se están utilizando. Si una cuenta de usuario o del sistema está inactiva durante un período determinado, siempre es mejor deshabilitar esa cuenta durante un período de tiempo determinado antes de eliminarla. Una vez que se elimina una cuenta, cualquier objeto que pertenezca a la cuenta puede volverse inaccesible. Tener este período en el que una cuenta está deshabilitada antes de la eliminación permite a los administradores identificar esos objetos y transferir su propiedad a otro usuario o cuenta del sistema.

Revocación de cuenta

La revocación de la cuenta, también conocida como desaprovisionamiento, es el proceso de eliminar una cuenta de un dispositivo o empresa. Debido a que a las cuentas se les asignan ID únicos en la mayoría de los sistemas operativos, es muy importante que los profesionales de seguridad se aseguren de que las cuentas ya no sean necesarias antes de eliminarlas. Existen innumerables historias en las que se eliminaron cuentas y luego se perdió el acceso a ciertos recursos. Incluso si un administrador vuelve a crear una cuenta con el mismo nombre de cuenta, no tendrá el mismo ID único que se asignó a la cuenta original. Por lo tanto, el administrador aún no podrá acceder a los recursos que pertenecen a la cuenta original.

Las organizaciones deben adoptar políticas formales sobre la revocación de cuentas. Estas políticas deben implementarse como parte de cualquier política de despido de empleados.

Amenazas de control de acceso

Las amenazas de control de acceso impactan directamente en la confidencialidad, integridad y disponibilidad de los activos organizacionales. El propósito de la mayoría de las amenazas de control de acceso es causar daño a una organización. Debido a que dañar a una organización es más fácil de hacer desde dentro de su red, los forasteros generalmente primero intentan atacar cualquier control de acceso que esté en su lugar.

Las amenazas de control de acceso que debe comprender incluyen

- Amenazas de contraseña
- Amenazas de ingeniería social
- DoS / DDoS
- Desbordamiento de búfer
- Código móvil
- Software malicioso
- Spoofing
- Olfatear y escuchar a escondidas
- Emanando
- Puerta trasera / trampilla

Amenazas de contraseña

Una amenaza de contraseña es cualquier ataque que intente descubrir las contraseñas de los usuarios. Las dos amenazas de contraseña más populares son los ataques de diccionario, los ataques de fuerza bruta, los ataques de cumpleaños, los ataques de tabla de arco iris y los ataques de rastreador.

Las mejores contramedidas contra las amenazas de contraseñas son implementar políticas de contraseñas complejas, exigir a los usuarios que cambien las contraseñas con regularidad, emplear políticas de bloqueo de cuentas, cifrar archivos de contraseñas y utilizar herramientas de descifrado de contraseñas para descubrir contraseñas débiles.

Ataque de diccionario

Un ataque de diccionario ocurre cuando los atacantes usan un diccionario de palabras comunes para descubrir contraseñas. Un programa automatizado usa el hash de la palabra del diccionario y compara este valor de hash con las entradas en el archivo de contraseña del sistema. Aunque el programa viene con un diccionario, los atacantes también usan diccionarios adicionales que se encuentran en Internet.

Debe implementar una regla de seguridad que diga que una contraseña NO debe ser una palabra encontrada en el diccionario para protegerse contra estos ataques. También puede implementar una política de bloqueo de cuenta para que una cuenta se bloquee después de una cierta cantidad de intentos de inicio de sesión no válidos.

Ataque de fuerza bruta

Los ataques de fuerza bruta son más difíciles de llevar a cabo porque funcionan a través de todas las combinaciones posibles de números y caracteres. Un ataque de fuerza bruta también esreferido como un ataque exhaustivo. Realiza búsquedas de contraseña hasta encontrar una contraseña correcta. Estos ataques también consumen mucho tiempo.

Ataque de cumpleaños

Un ataque de cumpleaños compara los valores que tiene un atacante con un conjunto de hashes de contraseñas cuyas contraseñas conoce. Finalmente, el atacante encontrará una contraseña que coincida. Para protegerse contra los ataques de cumpleaños, implemente el cifrado en la transmisión. El ataque recibe su nombre de la probabilidad de que los usuarios usen la misma contraseña, similar a la probabilidad de que los

usuarios tengan la misma fecha de cumpleaños, lo que a menudo se conoce como la paradoja del cumpleaños.

Ataque de mesa arcoiris

Un ataque de tabla de arco iris es similar a un ataque de cumpleaños en el sentido de que se utilizan comparaciones con valores hash conocidos. Sin embargo, en un ataque de arco iris, se utiliza una tabla de arco iris que contiene los valores hash criptográficos de las contraseñas. El uso de un algoritmo hash actualizado (frente a uno que está desactualizado) es el primer paso para protegerse contra este tipo de ataque. La salazón es el proceso de aleatorizar cada hash agregando datos aleatorios que son únicos para cada usuario a su hash de contraseña, por lo que incluso la misma contraseña tiene un hash único.

Ataque de rastreador

Un ataque de rastreador en el contexto de ataques de contraseñas simplemente utiliza un rastreador para capturar una contraseña sin cifrar o en texto plano. Los profesionales de la seguridad deben usar rastreadores periódicamente para ver si pueden determinar las contraseñas con estas herramientas. El cifrado de la transmisión de la contraseña lo impide.

Amenazas de ingeniería social

Los ataques de ingeniería social ocurren cuando los atacantes usan un lenguaje creíble y la credulidad del usuario para obtener credenciales de usuario o alguna otra información confidencial. Las amenazas de ingeniería social que debe comprender incluyen el phishing / pharming, la navegación lateral, el robo de identidad y el buceo en la basura.

La mejor contramedida contra las amenazas de ingeniería social es brindar capacitación a los usuarios sobre concientización sobre seguridad. Esta capacitación debe ser necesaria y debe ocurrir de manera regular porque las técnicas de ingeniería social evolucionan constantemente.

Phishing / Pharming

El phishing es un ataque de ingeniería social en el que los atacantes intentan obtener información personal, incluida la información de la tarjeta de crédito y los datos financieros. Este tipo de ataque se suele llevar a cabo mediante la implementación de un sitio web falso que se parece mucho a un sitio web legítimo. Los usuarios ingresan datos, incluidas las credenciales en el sitio web falso,permitiendo a los atacantes capturar cualquier información ingresada. El spear phishing es un ataque de phishing que se lleva a cabo contra un objetivo específico mediante el aprendizaje de los hábitos y gustos del objetivo. Los ataques de spear phishing tardan más en llevarse a cabo que los ataques de phishing debido a la información que se debe recopilar. La caza de ballenas es un tipo de phishing que se dirige específicamente a ejecutivos de alto nivel u otras personas de alto perfil. Vishing es un tipo de phishing que utiliza un sistema telefónico o tecnologías VoIP. El usuario recibe inicialmente una llamada, mensaje de texto o correo electrónico que le dice que llame a un número específico y proporcione información personal como nombre, fecha de nacimiento, número de seguro social e información de la tarjeta de crédito.

El pharming es similar al phishing, pero en realidad contamina el contenido de la caché de DNS de una computadora, de modo que las solicitudes a un sitio legítimo se enrutan a un sitio alternativo.

Advierta a los usuarios contra el uso de enlaces incrustados en mensajes de correo electrónico, incluso si el mensaje parece provenir de una entidad legítima. Los usuarios también deben revisar la barra de direcciones cada vez que acceden a un sitio donde se requiere su información personal para asegurarse de que el sitio sea correcto y de que se esté utilizando SSL, lo cual se indica mediante una designación HTTPS al comienzo de la dirección URL.

Hombro Surfeando

La navegación lateral ocurre cuando un atacante observa cuando un usuario ingresa un inicio de sesión u otros datos confidenciales. Anime a los usuarios a estar siempre al tanto de quién está observando sus acciones. La implementación de pantallas de privacidad ayuda a garantizar que la entrada de datos no se pueda registrar.

El robo de identidad

El robo de identidad ocurre cuando alguien obtiene información personal, incluido el número de licencia de conducir, número de cuenta bancaria y número de Seguro Social, y usa esa información para asumir la identidad de la persona cuya información fue robada. Una vez asumida la identidad, el ataque puede ir en cualquier dirección. En la mayoría de los casos, los atacantes abren cuentas financieras a nombre del usuario. Los atacantes también pueden obtener acceso a las cuentas válidas del usuario.

Buceo en contenedor

El buceo en basureros ocurre cuando los atacantes examinan el contenido de la basura para obtener información confidencial. Esto incluye información del personal, información de inicio de sesión de la cuenta, diagramas de red y datos financieros de la organización.

Las organizaciones deben implementar políticas para triturar documentos que contienen esta información.

DoS / DDoS

Un ataque de denegación de servicio (DoS) ocurre cuando los atacantes inundan un dispositivo con suficientes solicitudes para degradar el rendimiento del dispositivo objetivo. Algunos ataques DoS populares incluyen inundaciones SYN y ataques en forma de lágrima.

Un ataque DoS distribuido (DDoS) es un ataque DoS que se lleva a cabo desde múltiples ubicaciones de ataque. Los dispositivos vulnerables están infectados con agentes de software, llamados zombis. Esto convierte los dispositivos vulnerables en botnets, que luego llevan a cabo el ataque.

Debido a la naturaleza distribuida del ataque, identificar todas las botnets atacantes es prácticamente imposible. Las botnets también ayudan a ocultar la fuente original del ataque.

Desbordamiento de búfer

Los búferes son partes de la memoria del sistema que se utilizan para almacenar información. Se produce un desbordamiento del búfer cuando la cantidad de datos que se envían a la aplicación es mayor de lo que puede manejar el búfer. Normalmente, este tipo de ataque es posible debido a una aplicación o un código del sistema operativo mal escritos. Esto puede resultar en una inyección de código malicioso.

Para protegerse contra este problema, las organizaciones deben asegurarse de que todos los sistemas operativos y aplicaciones estén actualizados con los últimos service packs, actualizaciones y parches. Además, los programadores deben probar adecuadamente todas las aplicaciones para verificar si hay condiciones de desbordamiento. Finalmente, los programadores deben usar la validación de entrada para asegurarse de que los datos enviados no sean demasiado grandes para el búfer.

Código móvil

El código móvil es cualquier software que se transmite a través de una red para ejecutarse en un sistema local. Los ejemplos de código móvil incluyen subprogramas de Java, código de secuencia de comandos de Java y controles ActiveX. El código móvil incluye controles de seguridad, entornos sandbox de Java y firmas de código digital ActiveX. Se puede utilizar un código móvil malicioso para evitar los controles de acceso.

Las organizaciones deben asegurarse de que los usuarios comprendan las preocupaciones de seguridad del código móvil malicioso. Los usuarios solo deben descargar código móvil de sitios y proveedores legítimos.

Nota

Para obtener más información sobre el código móvil, consulte la sección " Código móvil " en el Capítulo 8 , " Seguridad del desarrollo de software ".

Software malicioso

El software malicioso, también llamado malware, es cualquier software diseñado para realizar actos maliciosos.

Las siguientes son las cinco clases de malware que debe comprender:

- **Virus :** cualquier malware que se adhiera a otra aplicación para replicarse o distribuirse.
- **Gusano :** cualquier malware que se replica a sí mismo, lo que significa que no necesita otra aplicación o interacción humana para propagarse.
- **Caballo de Troya :** cualquier malware que se disfrace de aplicación necesaria mientras realiza acciones maliciosas.
- **Spyware :** cualquier malware que recopile datos privados del usuario, incluido el historial de navegación o la entrada del teclado.
- **Ransomware :** cualquier malware que impide o limita el acceso de un usuario a su sistema o dispositivo. Por lo general, obliga a las víctimas a pagar el rescate por la devolución del acceso al sistema.

La mejor defensa contra el software malintencionado es implementar software antivirus y antimalware. Hoy en día, la mayoría de los proveedores empaquetan estos dos tipos de software en el mismo paquete. Mantener actualizado el software antivirus y antimalware es fundamental. Esto incluye asegurarse de que estén instaladas las últimas definiciones de virus y malware.

Spoofing

La suplantación, también conocida como enmascaramiento, ocurre cuando la comunicación de un atacante parece provenir de fuentes confiables. Los ejemplos de suplantación de identidad incluyen la suplantación de IP y la suplantación de hipervínculos. El objetivo de este tipo de ataque es obtener acceso a credenciales u otra información personal.

Un ataque de intermediario utiliza la suplantación de identidad como parte del ataque. Algunos profesionales de la seguridad consideran los ataques de phishing como un tipo de ataque de suplantación de identidad.

Olfatear y escuchar a escondidas

El olfateo, también conocido como espionaje, ocurre cuando un atacante inserta un dispositivo o software en el medio de comunicación que recopila toda la información transmitida a través del medio. Los rastreadores de red son utilizados tanto por profesionales de seguridad legítimos como por atacantes.

Las organizaciones deben monitorear y limitar el uso de rastreadores. Para protegerse contra su uso, debe cifrar todo el tráfico en la red.

Emanando

Las emanaciones son señales electromagnéticas emitidas por un dispositivo electrónico. Los atacantes pueden apuntar a ciertos dispositivos o medios de transmisión para espiar la comunicación sin tener acceso físico al dispositivo o medio.

El programa TEMPEST, iniciado por los Estados Unidos y el Reino Unido, investiga formas de limitar las emanaciones y estandariza las tecnologías utilizadas. Cualquier equipo que cumpla con los estándares TEMPEST suprime las emanaciones de señales utilizando material de protección. Los dispositivos que cumplen con los estándares TEMPEST generalmente implementan una barrera o revestimiento exterior, llamado jaula de

Faraday o escudo de Faraday. Los dispositivos TEMPEST se utilizan con mayor frecuencia en el gobierno, el ejército o las fuerzas del orden.

Puerta trasera / trampilla

Una puerta trasera o trampilla es un mecanismo implementado en muchos dispositivos o aplicaciones que le da al usuario que usa la puerta trasera acceso ilimitado al dispositivo o aplicación. Las cuentas de puerta trasera privilegiadas son el método más común de puerta trasera que verá hoy.

La mayoría de los proveedores establecidos ya no lanzan dispositivos o aplicaciones con este problema de seguridad. Debe conocer las puertas traseras conocidas en los dispositivos o aplicaciones que administra.

Agregación de acceso

La agregación de acceso es un término que se usa a menudo como sinónimo de arrastre de privilegios. La agregación de acceso se produce cuando los usuarios obtienen más acceso a más sistemas. Puede ser intencional, como cuando se implementa el inicio de sesión único, o no intencional, cuando a los usuarios se les otorgan más derechos sin tener en cuenta los derechos que ya tienen. El arrastre de privilegios o autorizaciones se produce cuando a los usuarios se les otorgan nuevos derechos sin que se revoquen los anteriores. Entonces, el arrastre de privilegios es en realidad un subconjunto de la agregación de acceso.

Para protegerse contra la agregación de acceso, las organizaciones deben implementar políticas de permisos / derechos que revisen una cuenta cuando se soliciten cambios de permisos o derechos. Los administradores deben asegurarse de que se eliminen todos los permisos o derechos existentes que el usuario ya no necesite. Por ejemplo, si un usuario pasa del departamento de contabilidad al departamento de ventas, la cuenta de usuario ya no debería tener permisos o derechos sobre los recursos contables.

Los profesionales de la seguridad deben trabajar con los propietarios y los custodios de los datos para garantizar que se implementen las políticas adecuadas.

Amenaza Persistente Avanzada

Una amenaza persistente avanzada (APT) es un ataque en el que una persona no autorizada obtiene acceso a una red y permanece durante un largo período de tiempo con la intención de robar datos. Una APT no tiene como objetivo causar daños a la red u organización. Su principal objetivo es acceder a información valiosa.

Una vez que el atacante obtiene acceso a la red, generalmente establece una puerta trasera. Para evitar el descubrimiento, el atacante reescribe el código y emplea sofisticadas técnicas de evasión. Algunas APT son tan complejas que requieren un administrador a tiempo completo. El atacante trabajará para establecer puertas traseras con cada violación exitosa de un sistema interno.

El mejor método para detectar APT es buscar anomalías o grandes cantidades de transferencias de datos en los datos salientes.

Prevenir o mitigar las amenazas de control de acceso

Debido a que las amenazas de control de acceso están tan extendidas, las organizaciones deben hacer todo lo posible para proteger sus sistemas de control de acceso, incluida la implementación de anti-malware, firewalls, detección y prevención de intrusiones y otras herramientas de defensa. Los profesionales de la seguridad deben alentar a sus organizaciones a implementar las siguientes medidas para prevenir o mitigar las amenazas de control de acceso:

- Implemente controles de acceso físico para todos los sistemas y dispositivos.

- Controle y supervise el acceso a los archivos de contraseñas.
- Cifre los archivos de contraseñas.
- Implemente una política de contraseñas seguras en toda la empresa.
- Implemente el enmascaramiento de contraseñas en todos los sistemas operativos y aplicaciones.
- Implemente la autenticación multifactor.
- Implementar bloqueo de cuenta.
- Implementar auditorías para controles de acceso.
- Implemente una política de administración de cuentas de usuario para garantizar que las cuentas de usuario se creen y eliminen según sea necesario.
- Brindar capacitación a los usuarios sobre concientización sobre seguridad que se centre específicamente en el control de acceso.

Tareas de preparación de exámenes

Como se menciona en la sección " Acerca de la *Guía de certificación CISSP* , tercera edición " en la Introducción, tiene un par de opciones para la preparación del examen: los ejercicios aquí, Capítulo 9 , " Preparación final " y las preguntas de simulación del examen en el Examen de Pearson. Software de preparación en línea.

Revisar todos los temas clave

Revise los temas más importantes de este capítulo, señalados con el icono de Temas clave en el margen exterior de la página. La Tabla 5-1 enumera una referencia de estos temas clave y los números de página en los que se encuentra cada uno.

Tabla 5-1 Temas clave para el Capítulo 5

Elemento de tema clave	Descripción	Número de página
Párrafo	Proceso de control de acceso	475
Lista	Cinco factores para la autenticación	484
Lista	Tipos de contraseñas	485
Lista	Consideraciones sobre la administración de contraseñas	486
Párrafo	Caracteristicas fisiologicas	490
Sección	Características de comportamiento	491
Sección	Consideraciones biométricas	492
Figura 5-1	Proceso de autenticación y registro biométrico	494
Liza	Ventajas y desventajas de SSO	499
Liza	Ventajas y desventajas de Kerberos	500
Figura 5-2	Proceso de emisión de tickets de Kerberos	501
Lista	Directrices del mecanismo de auditoría	506
Figura 5-3	Escenario ABAC básico NIST SP 800-162	511
Sección	Ciclo de vida de aprovisionamiento	514
Lista	Cinco clases de malware	521

Definir términos clave

Defina los siguientes términos clave de este capítulo y verifique sus respuestas en el glosario:

agregación de acceso

control de acceso

lista de control de acceso (ACL)

matriz de control de acceso

política de control de acceso

amenaza persistente avanzada (APT)

control de acceso basado en atributos (ABAC)

autenticación

autorización

Puerta trasera

aceptabilidad biométrica

precisión biométrica

tasa de rendimiento biométrico

ataque de cumpleaños

ataque de fuerza bruta

desbordamiento de búfer

tabla de capacidad

control de acceso centralizado

factores característicos

servicios de identidad en la nube

control de acceso dependiente del contexto

modelo de identidad federada de certificación cruzada

tasa de error cruzado (CER)

control de acceso descentralizado

autenticación de dispositivo

desaprovisionamiento

Ataque de diccionario

control de acceso discrecional (DAC)

contenedor de basura

tasa de aceptación falsa (FAR)

tasa de falso rechazo (FRR)

servicios de identidad federada

gestión de identidad federada (FIM)

identificación

Identidad como servicio (IDaaS)

Kerberos

factores de conocimiento

privilegios mínimos

Protocolo ligero de acceso a directorios (LDAP)

factores de ubicación

control lógico

control de acceso obligatorio (MAC)

autenticación multifactor

necesito saber

servicios de identidad locales

factores de propiedad

enmascaramiento de contraseña

pharming

suplantación de identidad

Control físico

privilegio arrastrarse

aprovisionamiento

ciclo de vida de aprovisionamiento

ataque de mesa arcoiris

Secuestro de datos

revocación

control de acceso basado en roles (RBAC)

control de acceso basado en reglas

Sistema europeo seguro para aplicaciones en un entorno de múltiples proveedores (SESAME)

Lenguaje de marcado de aserción de seguridad (SAML)

dominio de seguridad

separación de tareas

surf de hombro

autenticación de factor único

inicio de sesión único (SSO)

ataque de rastreador

software espía

trampilla

caballo de Troya

modelo de identidad federado de terceros de confianza

virus

vishing

ballenero

gusano

Responder preguntas de revisión

1 . ¿Cuál de los siguientes NO es un ejemplo de un factor de autenticación del conocimiento?

1. Clave
2. Nombre de soltera de la madre
3. Ciudad de nacimiento
4. Tarjeta electrónica

2 . ¿Cuál de las siguientes afirmaciones sobre tarjetas de memoria y tarjetas inteligentes es falsa?

1. Una tarjeta de memoria es una tarjeta magnética que contiene información de autenticación del usuario.
2. Las tarjetas de memoria también se conocen como tarjetas de circuito integrado (ICC).
3. Las tarjetas inteligentes contienen memoria y un chip integrado.
4. Los sistemas de tarjetas inteligentes son más confiables que los sistemas de tarjetas de memoria.

3 . ¿Qué método biométrico es más efectivo?

1. Escaneo de iris
2. Escaneo de retina
3. Huella dactilar
4. Impresión de mano

4 . ¿Qué es un error de tipo I en un sistema biométrico?

1. Tasa de error de cruce (CER)
2. Tasa de falso rechazo (FRR)
3. Tasa de aceptación falsa (FAR)
4. Tasa de rendimiento

5 . ¿Qué modelo de control de acceso utilizan con más frecuencia los enrutadores y firewalls para controlar el acceso a las redes?

1. Control de acceso discrecional
2. Control de acceso obligatorio
3. Control de acceso basado en roles
4. Control de acceso basado en reglas

6 . ¿Qué amenaza NO se considera una amenaza de ingeniería social?

1. Suplantación de identidad
2. Pharming
3. Ataque de DOS
4. Buceo en contenedor

7 . ¿Cuál de las siguientes afirmaciones describe mejor una implementación de IDaaS?

1. Garantiza que cualquier instancia de identificación y autenticación de un recurso se gestione correctamente.
2. Recopila y verifica información sobre una persona para demostrar que la persona que tiene una cuenta válida es quien dice ser.

3. Proporciona un conjunto de funciones de gestión de acceso e identidad para los sistemas de destino en las instalaciones de los clientes y / o en la nube.
4. Es un estándar SAML que intercambia datos de autenticación y autorización entre organizaciones o dominios de seguridad.

8 . ¿Cuál de los siguientes es un ejemplo de autenticación multifactor?

1. Nombre de usuario y contraseña
2. Nombre de usuario, escaneo de retina y tarjeta inteligente
3. Escaneo de retina y escaneo digital
4. Tarjeta inteligente y token de seguridad

9 . Decide implementar una política de control de acceso que requiere que los usuarios inicien sesión desde ciertas estaciones de trabajo dentro de su empresa. ¿Qué tipo de factor de autenticación está implementando?

1. Factor de conocimiento
2. Factor de ubicación
3. Factor de propiedad
4. Factor característico

10 . ¿Qué amenaza se considera una amenaza de contraseña?

1. Desbordamiento de búfer
2. Olfatear
3. Spoofing
4. Ataque de fuerza bruta

11 . ¿Qué mecanismos de administración de sesiones se utilizan a menudo para administrar sesiones de escritorio?

1. Salvapantallas y tiempos de espera
2. FIPS 201.2 y NIST SP 800-79-2
3. Bolardos y cerraduras

4. KDC, TGT y TGS

12 . ¿Cuál de las siguientes es una de las principales desventajas de implementar un sistema SSO?

1. Los usuarios pueden utilizar contraseñas más seguras.
2. Los usuarios deben recordar las credenciales de inicio de sesión para un solo sistema.
3. Se simplifica la administración de usuarios y contraseñas.
4. Si las credenciales de un usuario se ven comprometidas, un atacante puede acceder a todos los recursos.

13 . ¿Qué tipo de ataque se lleva a cabo desde múltiples ubicaciones utilizando zombies y botnets?

1. TEMPESTAD
2. DDoS
3. Puerta trasera
4. Emanando

14 . ¿Qué tipo de ataque es un ataque en el que una persona no autorizada accede a una red y permanece durante un largo período de tiempo con la intención de robar datos?

1. APTO
2. ABAC
3. Agregación de acceso
4. FIN

15 . ¿Cuál de los siguientes es un proceso formal para crear, cambiar y eliminar usuarios que incluye la aprobación de usuarios, la creación de usuarios, los estándares de creación de usuarios y la autorización?

1. NIST SP 800-63
2. Control de acceso centralizado
3. Control de acceso descentralizado

4. Ciclo de vida de aprovisionamiento

Respuestas y explicaciones

1 . D. Los factores de conocimiento son algo que una persona sabe, incluidas las contraseñas, el apellido de soltera de la madre, la ciudad de nacimiento y la fecha de nacimiento. Los factores de propiedad son algo que tiene una persona, incluida una tarjeta inteligente.

2 . B. Las tarjetas de memoria NO también se conocen como tarjetas de circuito integrado (ICC). Las tarjetas inteligentes también se conocen como ICC.

3 . un. Los escáneres del iris se consideran más efectivos que los escáneres de retina, huellas dactilares y huellas de manos.

4 . B. Un error de Tipo I en un sistema biométrico es la tasa de rechazo falso (FRR). Un error de Tipo II en un sistema biométrico es la tasa de aceptación falsa (FAR). La tasa de error de cruce (CER) es el punto en el que FRR es igual a FAR. La tasa de rendimiento es la tasa a la que se autentican los usuarios.

5 . D. El control de acceso basado en reglas es usado con mayor frecuencia por enrutadores y cortafuegos para controlar el acceso a las redes. Los otros tres tipos de modelos de control de acceso no suelen implementarse mediante enrutadores y cortafuegos.

6 . C. Un ataque de denegación de servicio (DoS) no se considera una amenaza de ingeniería social. Las otras tres opciones se consideran amenazas de ingeniería social.

7 . C. Una implementación de Identity as a Service (IDaaS) proporciona un conjunto de funciones de administración de identidad y acceso a los sistemas de destino en las instalaciones de los clientes y / o en la nube. La gestión de sesiones garantiza que cualquier instancia de identificación y

autenticación de un recurso se gestione correctamente. Un proceso de prueba de identidad recopila y verifica información sobre una persona para demostrar que la persona que tiene una cuenta válida es quien dice ser.

8 **. B.** El uso de nombre de usuario, escaneo de retina y una tarjeta inteligente es un ejemplo de autenticación multifactor. El nombre de usuario es algo que conoce, el escaneo de retina es algo que usted es y la tarjeta inteligente es algo que tiene.

9 **. B.** Está implementando un factor de ubicación, que se basa en la ubicación de una persona al iniciar sesión.

10 **. D.** Un ataque de fuerza bruta se considera una amenaza de contraseña.

11 **. un.** Las sesiones de escritorio se pueden administrar a través de protectores de pantalla, tiempos de espera, inicio de sesión y limitaciones de programación. FIPS PUB 201.2 y NIST SP 800-79-2 son documentos que brindan orientación sobre la prueba de identidad. El acceso físico a las instalaciones se puede proporcionar de forma segura mediante cerraduras, cercas, bolardos, guardias y CCTV. En Kerberos, el Centro de distribución de claves (KDC) emite un vale de concesión de tickets (TGT) al principal. El principal envía el TGT al servicio de concesión de tickets (TGS) cuando el principal necesita conectarse a otra entidad.

12 **. D.** Si las credenciales de un usuario se ven comprometidas en un entorno de inicio de sesión único (SSO), los atacantes tienen acceso a todos los recursos a los que tiene acceso el usuario. Todas las demás opciones son ventajas para implementar un sistema SSO.

13 **. B.** Un ataque DoS distribuido (DDoS) es un ataque DoS que se lleva a cabo desde múltiples ubicaciones de ataque. Los dispositivos vulnerables están infectados con agentes de software, llamados zombis. Esto convierte los dispositivos vulnerables en botnets, que luego llevan a cabo

el ataque. Los dispositivos que cumplen con los estándares TEMPEST implementan una barrera o revestimiento exterior, llamado jaula de Faraday o escudo de Faraday. Una puerta trasera o trampilla es un mecanismo implementado en muchos dispositivos o aplicaciones que le da al usuario que usa la puerta trasera acceso ilimitado al dispositivo o aplicación. Las emanaciones son señales electromagnéticas emitidas por un dispositivo electrónico. Los atacantes pueden apuntar a ciertos dispositivos o medios de transmisión para espiar la comunicación sin tener acceso físico al dispositivo o medio.

14 . un. Una amenaza persistente avanzada (APT) es un ataque en el que una persona no autorizada obtiene acceso a una red y permanece durante un largo período de tiempo con la intención de robar datos. El control de acceso basado en atributos (ABAC) otorga o niega las solicitudes de los usuarios en función de atributos arbitrarios del usuario y atributos arbitrarios del objeto, y las condiciones ambientales que pueden ser reconocidas globalmente. La agregación de acceso es un término que se usa a menudo como sinónimo de arrastre de privilegios. La agregación de acceso se produce cuando los usuarios obtienen más acceso a más sistemas. En la gestión de identidad federada (FIM), cada organización que se une a la federación acepta hacer cumplir un conjunto común de políticas y estándares. Estas políticas y estándares definen cómo aprovisionar y administrar la identificación, autenticación y autorización de usuarios.

15 . D. El ciclo de vida de aprovisionamiento es un proceso formal para crear, cambiar y eliminar usuarios. Este proceso incluye la aprobación de usuarios, la creación de usuarios, los estándares de creación de usuarios y la autorización. Los usuarios deben firmar una declaración escrita que explique las condiciones de acceso, incluidas las responsabilidades del usuario. NIST SP 800-63 proporciona un conjunto de requisitos técnicos para las agencias federales que implementan servicios de identidad digital, incluida una descripción general de los marcos de identidad; utilizando autenticadores, credenciales y afirmaciones en sistemas

digitales. En el control de acceso centralizado, un departamento o personal central supervisa el acceso de todos los recursos de la organización. Este método de administración garantiza que el acceso de los usuarios se controle de manera coherente en toda la empresa. En el control de acceso descentralizado, el personal más cercano a los recursos.